IBM Parallel System Support Programs for AIX Installation and Migration Guide

Document Number GC23-3898-02

Note!

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

Second Edition (November 1996)

This is a major revision of GC23-3898-02.

This edition applies to Version 2 Release 2 of IBM Parallel System Support Programs for AIX (5765-529), which runs on IBM RS/6000 Scalable POWERparallel Systems, 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.

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 1996. 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 xi
Trademarks xi
Publicly Available Software xii

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

Chapter 1. Overview of the RS/6000 SP Installation Process 1
What's New in PSSP and AIX? 1
Installing Your SP System 3
Prepare and Install the Control Workstation 4
Enter Node and Configuration Information 4
Install SP on the Nodes (Externals) 4
Install SP on the Nodes (Internals) 5
Working With the Basic AIX Image 8
Building a New AIX 4.1 Image 8
Detailed Overview of Network Installation of a Node 9
Network Installation 9

Chapter 2. Installing and Configuring a New RS/6000 SP System 13
Finding Related Installation Information 13
Task A. Prepare the Control Workstation 14

© Copyright IBM Corp. 1996

Step 1: Update the root User Path . . . 14
Step 2: Verify the Control Workstation Requirements . . . 14
Step 3: Verify Network Requirements . . . 15
Step 4: Connect Frames to Your Control Workstation . . . 15
Step 5: Configure RS-232 Control Lines . . . 15
Step 6: Tune the Network Adapters . . . 16
Step 7: Configure 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 root Maximum Default Processes . . . 18
Step 11: Change Tunables and Tunable Values . . . 19
Step 12: Define Space for NIM Boot Images . . . 20
Step 13: Define Space for the /spdata Directory . . . 21
Step 14: Create Required /spdata Directories . . . 23
Step 15: Copy the AIX 4.1 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: Install a Basic AIX (mksysb) Image . . . 27
Step 18: Install PSSP on the Control Workstation . . . 27
Step 19: Customize the script.cust and tuning.cust Files . . . 30
Step 20: Initialize RS/6000 SP Authentication Services . . . 30
Step 21: Complete System Support Installation on the Control Workstation 39
Step 22: Run SDR and System Monitor Verification Tests . . . 40
Task C. Enter Site Environment, Frame, Node, and Switch Information . . . 41
Step 23: Enter Site Environment Information . . . 41
Step 24: Enter Frame Information and Reinitialize the SDR . . . 42
Step 25: Start System Partition-Sensitive Subsystems . . . 43
Step 26: Verify System Partition-Sensitive Subsystems Have Started . . . 44
Step 27: Verify System Monitor Installation . . . 45
Step 28: Verify Frame Information . . . 45
Step 29: Update the State of the Supervisor Microcode . . . 46
Step 30: Enter Required Node Information . . . 47
Step 31: Acquire Hardware Ethernet Addresses . . . 49
Step 32: Verify Ethernet Addresses Were Acquired . . . 51
Step 33: Configure Additional Adapters for Nodes . . . 51
Step 34: Configure Initial Host Names for Nodes . . . 56
Step 35: Set Up Nodes to Be Installed . . . 57
Step 36: Verify All Node Information . . . 60
Step 37: Configure Control Workstation as Boot/Install Server . . . 62
Task D. Power On and Install the Nodes . . . 63
Step 38: Perform Additional Node Customization . . . 63
Step 39: Verify the System Management Tools Were Correctly Installed . . . 63
Step 40: Set Up the Switch . . . 64
Step 41: Verify the Switch Primary and Primary Backup Nodes . . . 67
Step 42: Set Switch Clock Source for All Switches . . . 68
Step 43: Set Up System Partitions . . . 69
Step 44: Network Boot Optional Boot/Install Servers . . . 70
Step 45: Verify that System Management Tools Were Correctly Installed on Boot/Install Servers . . . 75
Step 46: Network Boot the Remaining RS/6000 SP Nodes . . . 75
Step 47: Verify Node Installation . . . 76
Step 48: Run Verification Tests on All Nodes . . . 78
Step 49: Start the Optional Switch . . . 78
Step 50: Verify the Switch Was Installed Correctly . . . 79

Step 51: Tune the Network Adapters 81
Run Postinstallation Procedures 82

Chapter 3. Installing and Configuring the High Availability Control Workstation 83
Finding Related Installation Information 84
Task A: Prepare the Control Workstations 85
Step 1: Understand the Procedure 85
Step 2: Plan Network Configuration 85
Step 3: Install the SP System 89
Step 4: Install AIX on the Backup Control Workstation 90
Step 5: Back Up the Control Workstations 90
Step 6: Set Up the Hardware 90
Step 7: Configure RS-232 Control Lines 90
Task B. Update RS/6000 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 104
Step 27: Make Each Control Workstation Addressable by its Hostname . 104
Step 28: Set Up the HACWS Configuration 104
Step 29: Customize Cluster Event Processing 105
Step 30: Add IP Address Aliases 105
Step 31: Verify the HACWS Configuration 105
Step 32: Verify the Hardware Connections 106
Step 33: Reboot Control Workstations 106
Step 34: Start Cluster Services on the Primary Control Workstation 106
Step 35: Verify HACWS Installation 106

Chapter 4. Migrating to the Latest Level of PSSP 109
Preparing to Migrate 109
Steps to Migrate the Control Workstation from PSSP 1.2 to PSSP 2.2 109
Step 1: Back Up Your Control Workstation 110
Step 2: Back Up Important File Systems on the Control Workstation . . . 111

Step 3: Prepare AIX 3.2.5 Boot Install and /usr Servers 111
Step 4: Verify the Control Workstation Requirements 112
Step 5: Prepare for PSSP Installation 112
Step 6: Prepare for PSSP Migration Installation 113
Step 7: Perform BOS Migration Installation on the Control Workstation . . 113
Step 8: Prepare for PSSP Reinstallation 114
Step 9: Perform BOS Install on the Control Workstation 116
Step 10: Restore Configuration Files 117
Step 11: Restore Additional Configuration Files 117
Step 12: Configure RS-232 Control Lines 117
Step 13: Configure Ethernet Adapters 118
Step 14: Verify Control Workstation Interfaces 119
Step 15: Define Space for NIM Boot Images 119
Step 16: Define Space for the /spdata Directory 120
Step 17: Copy the AIX 4.1 LPP Images 121
Step 18: Copy the PSSP Images 121
Step 19: Install the Basic AIX Image 121
Step 20: Install PSSP on the Control Workstation 121
Step 21: Authenticate as the Administrative Principal 121
Step 22: Complete PSSP Installation on the Control Workstation 121
Step 23: Run SDR and System Monitor Verification Test 121
Step 24: Configure PSSP Services 121
Step 25: Set Up the Site Environment LPP Source Name 122
Step 26: Start System Partition-Sensitive Subsystems 122
Step 27: Verify System Partition-Sensitive Subsystems Have Started . . . 122
Step 28: Validate the Upgraded Control Workstation 122
Step 29: Shut Down the Nodes 122
Step 30: Create System Partitions 123
Step 31: Reboot the Nodes in the Production System Partition 123
Step 32: Install AIX 4.1 and PSSP 2.2 in the Test System Partition 123
Step 33: Test PSSP 2.2 124
Steps to Migrate the Control Workstation from PSSP 2.1 to PSSP 2.2 125
Step 1: Archive the SDR (optional) 126
Step 2: Back Up Your Control Workstation 126
Step 3: Back Up Important File Systems on the Control Workstation . . . 126
Step 4: Verify the Control Workstation Requirements 126
Step 5: Prepare for PSSP Installation 126
Step 6: Prepare for PSSP Reinstallation 127
Step 7: Perform BOS Install on the Control Workstation 129
Step 8: Restore Configuration Files 129
Step 9: Restore /spdata 130
Step 10: Restore Additional Configuration Files 130
Step 11: Configure RS-232 Control Lines 130
Step 12: Configure Ethernet Adapters 130
Step 13: Verify Control Workstation Interfaces 131
Step 14: Review Space Requirements for NIM Boot Images 131
Step 15: Review Space Requirements for /spdata 132
Step 16: Create Required /spdata Directories 132
Step 17: Review the AIX 4.1.4 LPP Images 132
Step 18: Move the Existing LPP Images 133
Step 19: Copy the PSSP Images for PSSP 2.2 133
Step 20: Move the PSSP Images for PSSP 2.1 133
Step 21: Install the Basic AIX Image 134
Step 22: Stop Daemons on the Control Workstation 134

Step 23: Verify that the Daemons are Not Running 134
Step 24: Install PSSP on the Control Workstation 134
Step 25: Authenticate as the Administrative Principal 134
Step 26: Complete PSSP Installation on the Control Workstation 134
Step 27: Run SDR and System Monitor Verification Test 134
Step 28: Configure PSSP Services 135
Step 29: Set Up the Site Environment LPP Source Name 135
Step 30: Start System Partition-Sensitive Subsystems 135
Step 31: Verify System Partition-Sensitive Subsystems Have Started . . . 135
Step 32: Unconfigure the NIM Master 135
Step 33: Configure Control Workstation as Boot/Install Server 135
Step 34: Validate the Upgraded Control Workstation 136
Step 35: Shut Down the Nodes 136
Step 36: Create System Partitions 136
Step 37: Reboot the Nodes in the Production System Partition 136
Step 38: Install AIX 4.1 and PSSP 2.2 in the Test System Partition 136
Step 39: Test PSSP 2.2 137
Strategy for HACWS Migration 138
Migrating an HACWS Configuration from PSSP 2.1 to PSSP 2.2 139
Step 1: Back Up Your HACWS Configuration 139
Step 2: Back Up Important File Systems on the Control Workstations . . 139
Step 3: Install AIX 4.1.4 on Both Control Workstations 139
Step 4: Install HACMP 4.2 on Both Control Workstations 139
Step 5: Create Required /spdata Directories 140
Step 6: Copy the AIX 4.1.4 LPP Images to the Control Workstation . . . 140
Step 7: Move the Existing LPP Images 140
Step 8: Copy the PSSP 2.2 Images 140
Step 9: Move the PSSP 2.1 Images 140
Step 10: Install the Basic AIX Image 140
Step 11: Start Control Workstation Services on Primary Control Workstation 140
Step 12: Stop Control Workstation Services While HACMP is Running . . 140
Step 13: Install PSSP 2.2 on Both Control Workstations 140
Step 14: Authenticate as the Administrative Principal 141
Step 15: Complete PSSP 2.2 Installation on Both Control Workstations . 141
Step 16: Verify the HACWS Configuration 141
Step 17: Run SDR and System Monitor Verification Tests 141
Step 18: Set Up the Site Environment LPP Source Name 141
Step 19: Unconfigure the NIM Master 141
Step 20: Restart Control Workstation Services 141
Migrating Nodes from PSSP 1.2 to PSSP 2.2 142
Steps to Migrate Nodes from PSSP 1.2 to PSSP 2.2 142
Step 1: Set Up the lpp_source and PSSP Code Version 142
Step 2: Set the Node(s) to Migrate 142
Step 3: Verify Boot Setup 143
Step 4: Run setup_server to configure the changes. 143
Step 5: Network Boot the Node or Nodes 143
Step 6: Wait for Network Boot to Finish 143
Step 7: Refresh System Partition-Sensitive Subsystems 143
Migrating Nodes from PSSP 2.1 to PSSP 2.2 144
Steps to Migrate Nodes from PSSP 2.1 to PSSP 2.2 144
Step 1: Upgrade the Node or Nodes to AIX 4.1.4 144
Step 2: Set Up the lpp_source and PSSP Code Version 144
Step 3: Set the Node or Nodes to Customize 145

Step 4: Verify Boot Setup . . . 145
Step 5: Run setup_server to Configure the Changes . . . 145
Step 6: Copy the PSSP 2.2 pssp_script to Nodes' /tmp . . . 145
Step 7: Execute the pssp_script on the Node(s) . . . 145
Step 8: Wait for pssp_script to Finish . . . 145
Step 9: Start System Partition-Sensitive Subsystems . . . 145
Step 10: Refresh System Partition-Sensitive Subsystems . . . 146
Steps to Do an Overwrite Install to Upgrade to PSSP 2.2 . . . 146
Step 1: Set Up the lpp_source and PSSP Code Version . . . 146
Step 2: Set the Node(s) to Install . . . 146
Step 3: Verify Boot Setup . . . 146
Step 4: Run setup_server to configure the changes. . . . 147
Step 5: Network Boot the Node or Nodes . . . 147
Step 6: Wait for Network Boot to Finish . . . 147
Step 7: Refresh Partition-Sensitive Subsystems . . . 147
Coexistence with PSSP 2.2 and Earlier Releases . . . 148

Chapter 5. Reconfiguring the RS/6000 SP System . . . 149
Adding a Frame . . . 150
Step 1: Connect Frames to Your Control Workstation . . . 150
Step 2: Power On Frames and Switches . . . 150
Step 3: Configure the RS-232 Control Line . . . 150
Step 4: Configure the Ethernet Adapter (Optional) . . . 151
Step 5: Enter Frame Information and Reinitialize the SDR . . . 151
Step 6: Verify Frame Information . . . 151
Step 7: Update the State of the Supervisor Microcode . . . 151
Step 8: Add Nodes to the System . . . 151
Step 9: Refresh System Partition-Sensitive Subsystems . . . 152
Step 10: Stop and Restart the Resource Manager in all Affected Partitions 152
Deleting a Frame . . . 152
Step 1: Stop the Resource Manager Server . . . 153
Step 2: Shut Down All the Nodes in the Partition . . . 153
Step 3: Delete Frame Information from the SDR . . . 154
Step 4: Reconfigure the System Partitions (Optional) . . . 154
Step 5: Refresh System Partition-Sensitive Subsystems . . . 154
Step 6: Restart the SP System Monitor GUI and Perspectives . . . 154
Step 7: Restart the Resource Manager Server . . . 155
Adding Nodes . . . 155
Step 1: Connect New Nodes to the Frame . . . 156
Step 2: Update the State of the Supervisor Microcode . . . 156
Step 3: Set Up, Power, and Configure the Nodes . . . 156
Step 4: Refresh System Partition-Sensitive Subsystems . . . 156
Step 5: Restart System Monitor GUI and Perspectives . . . 156
Step 6: Stop and Restart the Resource Manager Server . . . 156
Deleting Nodes . . . 157
Step 1: Stop the Resource Manager Server . . . 157
Step 2: Shut Down the Nodes . . . 158
Step 3: Disconnect the Node from the Frame . . . 158
Step 4: Delete Node Information From the SDR . . . 158
Step 5: Refresh System Partition-Sensitive Subsystems . . . 159
Step 6: Restart the Resource Manager Server . . . 159
Replacing a Node with an Equivalent Node . . . 159
Step 1: Shut Down the Node and Power It Off . . . 160
Step 2: Replace the Old Node with the New One and Power It On . . . 160

Step 3: Update the State of the Supervisor Microcode 160
Step 4: Delete NIM Client 160
Step 5: Acquire the Hardware Ethernet Address 161
Step 6: Set Up Nodes To Be Installed 161
Step 7: Restart Perspectives 161
Step 8: Network Boot the New SP Node 161
Step 9: Run Post—installation Procedures 162
Replacing a Node with a Different Type of Node 162
Step 1: Shut Down the Node and Power It Off 162
Step 2: Disconnect the Node From the Frame 163
Step 3: Stop the Resource Manager Server 163
Step 4: Delete Node Information From the SDR 164
Step 5: Replace the Old Node with the New One and Power It On 164
Step 6: Delete NIM Client 164
Step 7: Update the State of the Supervisor Microcode 164
Step 8: Set Up, Power, and Configure the Nodes 164
Step 9: Refresh System Partition-Sensitive Subsystems 165
Step 10: Restart the Resource Manager Server 165
Adding a Switch 165
Adding a Switch to a Switchless System 166
Adding a Switch to a System With Existing Switches 168
Reconfiguring Your System for Use with the SP Switch 169
Prerequisites to Transferring Switches 169
Step 1: Prepare for the Switch Transfer 169
Step 2: Shut Down All Nodes and Clean Up the Control Workstation . . . 170
Step 3: Replace the High Performance Switch and Switch Adapters . . . 171
Step 4: Reconfigure the Hardware Monitor to Recognize New Hardware . 171
Step 5: Update the State of the Supervisor Microcode 172
Step 6: Update the System Data Repository 172
Step 7: Annotate a Switch Topology File 172
Step 8: Set the Switch Primary and Primary Backup Nodes 173
Step 9: Set Switch Clock Source for All Switches 174
Step 10: Set Up Nodes to Customize 175
Step 11: Power On the Nodes 176
Step 12: Verify SP Switch Adapters 176
Step 13: Start the Switch 177
Step 14: Run Verification Test on the Switch 178
Step 15: Reapply System Partition Configuration 178
Replacing the Frame Supervisor 178
Step 1: Install the New Frame Supervisor Card 178
Step 2: Reconfigure the Hardware Monitor to Recognize New Hardware . 178
Step 3: Update the State of the Supervisor Microcode 178
Step 4: Issue Eannotate 178
Step 5: Issue Eclock 178
Replacing a Fixed Disk 179
Step 1: Power Off the Node 179
Step 2: Replace the Disk 179
Step 3: Install the System Image on the Disk 179
Step 4: Network Boot the Node 180
Replacing a Disk Not in rootvg 180
Step 1: Power Off the Node 180
Step 2: Replace the Failing Fixed Disk 181
Step 3: Power On the Node 181
Step 4: Restore Any Data Previously Backed-Up 181

Replacing an I/O Planar Card in a Thin Node or an Ethernet Adapter in a Wide or 604 High Node . . . 181
Step 1: Power Off the Node . . . 182
Step 2: Replace the Card . . . 182
Step 3: Delete NIM Client . . . 182
Step 4: Obtain the New Hardware Ethernet Address . . . 182

Chapter 6. Performing Software Maintenance . . . 183
Installing Program Updates . . . 183
Which Approach is Right for You? . . . 184
Working With Nodes That Are Down . . . 184
Reinstalling PSSP . . . 185
Updating the css Option . . . 185
Updating the Print Subsystem . . . 185
Installing Updates on a Per Node Basis . . . 185
Installing Updates through Reinstallation . . . 186
Build an Installation Image . . . 186
Test Your Image on a Single Node . . . 187
Propagate Your Installation Image . . . 187
Applying PTFs to the SP System . . . 188
Task A: Prepare the Control Workstation . . . 188
Task B: Apply PTFs on One SP Node and Verify Correct Operation . . . 189
Task C: Apply PTFs to All Nodes . . . 189
Task D: Commit PTFs on Node and Control Workstation . . . 189
Task E: Update the State of the Supervisor Microcode . . . 190
Task F: Create New mksysb Images . . . 190
Restoring a Control Workstation from mksysb Image . . . 190

Appendix A. SP Perspectives and System Monitor GUI Tasks . . . 191
Starting and Using Perspectives . . . 191
Starting and Using the System Monitor Graphical User Interface . . . 191

Appendix B. Directory Information . . . 195

Appendix C. Sample script.cust File . . . 197

Appendix D. Sample tuning.cust File . . . 203

Appendix E. SAGE Job Descriptions . . . 205
Core Templates Defined by SAGE . . . 205
Junior System Administrator . . . 205
Intermediate/Advanced System Administrator . . . 206
Additional Skill Areas . . . 206

Appendix F. Boot/Install Server Configuration Commands . . . 209

Glossary of Terms and Abbreviations . . . 211

Index . . . 219

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
AIX/6000
DATABASE 2
ES/9000
ESCON
HACMP/6000
IBM
IBMLink
InfoExplorer
LoadLeveler
Micro Channel
NQS/MVS
POWERparallel
POWERserver
POWERstation
RISC System/6000
RS/6000
Scalable POWERparallel Systems
SP1
SP2

© Copyright IBM Corp. 1996

System/370 TURBOWAYS
System/390

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:

Amd Berkeley Software Distribution automount daemon

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, and maintain 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.

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

- The *IBM Parallel System Support Programs for AIX: System Planning* 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 pertaining to:
  - Understanding IBM RS/6000 Scalable POWERparallel Systems (SP)
  - Performing routine system administration tasks
  - Making the system secure
  - Managing sets of nodes
  - Monitoring the system
  - Providing for system availability and problem management
  - Tuning the system
- The *IBM Parallel System Support Programs for AIX: Installation and Migration Guide* helps you understand and perform SP installation, configuration, maintenance, and migration. It includes concepts and instructions for:
  - Installing and configuring the IBM Parallel System Support Programs (PSSP) for AIX
  - Migrating to PSSP Version 2 Release 2
  - Reconfiguring the system
  - Performing system maintenance
- 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 2. To find out what version of PSSP is running on your system, enter the following:

```
SDRGetObjects Syspar syspar_name code_version
```

In response, the system displays something similar to:

```
syspar_name  code_version
Part_1       PSSP-2.2
```

© Copyright IBM Corp. 1996

If the response indicates **PSSP-2.2**, this book applies to the version of PSSP that is running on your system.

If you are running mixed levels of PSSP in a system partition, be sure to maintain and refer to the appropriate documentation for whatever versions of PSSP you are running. this book applies to the version of PSSP that is running on your system.

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 Guide 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 level III skills (Intermediate/Advanced System Administrator) depending on the complexity of your site and system. See Appendix E, “SAGE Job Descriptions” on page 205 for more information on these job skills.

How This Book Is Organized

- Chapter 1, “Overview of the RS/6000 SP Installation Process” 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 set up and functioning in your environment.
- Chapter 3, “Installing and Configuring the High Availability Control Workstation” on page 83 explains how to setup and configure your optional high availability cluster multi-processing.
- Chapter 4, “Migrating to the Latest Level of PSSP” on page 109 describes how to install PSSP V2R1 on a system that is already running PSSP V1R2.
- Chapter 5, “Reconfiguring the RS/6000 SP System” on page 149 discusses adding and replacing hardware components.
- Chapter 6, “Performing Software Maintenance” on page 183 provides information on updating installatiom images, LPPs, and support programs.
- Appendix A, “SP Perspectives and System Monitor GUI Tasks” on page 191 provides instructions for completing common tasks using SP Perspectives and the System Monitor graphical user interface.
- Appendix B, “Directory Information” on page 195 contains a list of the directories created when you install the RS/6000 SP LPP image.
- Appendix C, “Sample script.cust File” on page 197 contains a sample boot customization file (**script.cust**).
- Appendix D, “Sample tuning.cust File” on page 203 contains a sample tuning customization file (**tuning.cust**).

- Appendix E, “SAGE Job Descriptions” on page 205 contains system administrator job descriptions defined by SAGE.

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**>.

Obtaining Documentation

This book is available in PostScript format. You can obtain PostScript files for the product documentation by:

- Downloading them from the **lscftp.pok.ibm.com** anonymous FTP server. The files for PSSP can be found in the directory called /**pub**/**pps**/**pssp**.
- Printing the PostScript documentation files that are shipped on the product media.

You can also view or download this book from the IBM RS/6000 web site at **http://www.rs6000.ibm.com**.

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

The system response to an action follows the ▲ symbol.

▲ The diagnostic display appears.

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 installation and migration 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, type **spmon -g**

Related Publications

SP Hardware Publications

- *IBM RS/6000 Scalable POWERparallel Systems: Site Planning*, GC23-3905
- *IBM RS/6000 Scalable POWERparallel Systems: Maintenance Information, Volume 1, Installation and CE Operations*, GC23-3903
- *IBM RS/6000 Scalable POWERparallel Systems: Maintenance Information, Volume 2, Maintenance Analysis Procedures and Parts Catalog*, GC23-3904
- *IBM RS/6000 Scalable POWERparallel Systems: Library Guide*, GC23-3868
- *IBM RS/6000 Scalable POWERparallel Systems: Installation Aid Licensed Program Specification*, GC23-3838

SP Software Publications

- *IBM Parallel System Support Programs for AIX: Administration Guide*, GC23-3897
- *IBM Parallel System Support Programs for AIX: Installation and Migration Guide*, GC23-3898
- *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 Publications

- *IBM Parallel System Support Programs for AIX: Managing Shared Disks: IBM Virtual Shared Disks, Data Striping Devices, and the IBM Recoverable Virtual Shared Disk Licensed Program*, SC23-3849
- *IBM Recoverable Virtual Shared Disk: Licensed Program Specification*, GC23-3848

Performance Monitor Publication

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

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

AIX and RISC System/6000 Publications

- *IBM AIX Version 4 Getting Started*, SC23-2527
- *IBM 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
- *IBM AIX Versions 3.2 and 4 Performance Tuning Guide*, SC23-2365
- *IBM AIX Version 4 Problem Solving Guide and Reference*, SC23-2606
- *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

- *RS/6000 Problem Solving Guide*, SC23-2204
- *Common Diagnostics Micro Channel*, SA23-2765
- *7012 300 Series Operator Guide*, SA23-2623
- *7012 300 Series Installation and Service Guide*, SA23-2624
- *7013 500 Series Operator Guide*, SA23-2621
- *7013 500 Series Installation and Service Guide*, SA23-2622
- *Electrical Safety for IBM Service Representatives*, S229-8124
- *Service Information Binder*, SX33-6060
- *7015 Model R30 CPU Operator Guide*, SA23-2742
- *7015 Model R30 CPU 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

- *FDDI Introduction and Planning Guide*, GA27-3892
- *FDDI User's Guide and Programming Reference*, SC28-2823
- *Block Multiplexer Channel Adapter User's Guide and Service Information*, SC23-2427
- *Planning for Fiber Optic Channel Links*, GA23-0367
- *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 SCSI Model 010 Expansion Unit: Installation and Service Guide*, SY33-0165
- *9334 SCSI Model 500 Expansion Unit: 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*. Adison Wesley, 1995.
- Bergmark, D., Pottle, M. *Optimization and Parallelization of a Commodity Trade Model for the SP1*. Cornell Theory Center, Cornell University, June, 1994.
- Phister, 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.

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
Amd	/usr/lpp/ssp/man/man8/amd.8
	/usr/lpp/ssp/man/man8/amq.8
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 5.002)	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 RS/6000 SP Installation Process

This chapter provides an overview of the installation process and describes what happens during system installation.

Before you install the SP system, you must perform several planning activities. These activities include completing worksheets or checklists that reflect your decisions regarding:

- Device support
- System partitioning
- Network connections
- Node and switch configuration
- System management options
- Boot/Install Server and node relationships
- Location and type of authentication servers.

Note

It is essential that you plan your system carefully before attempting to install it. Refer to the *System Planning Guide* for planning details.

What's New in PSSP and AIX?

AIX 4.1.4

AIX 4.1.4 is a service level update to AIX 4.1. For information on AIX 4.1, 4.1.4, or higher service levels, refer to the AIX documentation.

PSSP 2.2

The new function in PSSP 2.2 requires AIX level 4.1.4 or greater.

604 High Node Support: The 604 high node introduces Symmetric Multi-Processor and PowerPC technology to the RS/6000 Scalable POWERparallel Systems computer. System management support is provided that allows the 604 high node to be managed in a way that is consistent with the management of the thin and wide nodes. In addition, support for the new node is provided by the System Partitioning Aid, the IBM Virtual Shared Disk, and the SP Switch.

The System Partitioning Aid: PSSP provides a set of predefined system partition layouts. If one of these predefined layouts does not meet your needs, you can use the System Partitioning Aid to create and save a new one. When the system administrator accepts a system partition layout generated by the System Partitioning Aid, the tool generates the topology files, node lists, and layout descriptions and saves the configuration in the system partitioning directory structure.

The System Partitioning Aid can be invoked from a command line interface or from the new graphical user interface called Perspectives.

Perspectives: Scalable POWERparallel Perspectives for AIX is a graphical user interface that enables you to perform system management tasks for your RS/6000 Scalable POWERparallel Systems computer through direct manipulation of system

© Copyright IBM Corp. 1996

objects represented by icons. You can use this GUI to perform system management tasks such as monitoring and controlling hardware, creating system events, defining and managing IBM Virtual Shared Disks, and configuring system partitions.

Installation Support: PSSP 2.2 provides the ability to install multiple versions of AIX and PSSP from a single node or the control workstation; the clients must be at AIX 4.1 and PSSP 2.1 or later. It provides a set of new installation commands which provide a greater flexibility in installation error recovery. An AIX 4.1 boot install node has Network Installation Manager (NIM) support to allow an AIX migration install from AIX 3.2.5 to AIX 4.1.

Node Grouping: Function is provided to persistently name a set of nodes which can then be acted on as a single entity or object. Node groups can be created, modified, and deleted through a command line interface or through Perspectives. They can also be used by other PSSP commands or imbedded in shell scripts.

Problem Management: Problem Management enables the easy exploitation of Event Management services. By entering simple commands, an administrator may subscribe events such as nodes down, reaching a filesystem threshold, high paging rates, and so on, and may associate these commands or scripts to be triggered by events, such as recovery steps or mailing messages. This infrastructure may be used to make an application highly available by providing automatic recovery from subscribed events. Problem Management also enables the user to create resource monitors, special user programs which monitor specialized resources. Problem management will check the output of these monitors, and generate events on special (user-defined) conditions. This feature is especially valuable in making an application highly available, since a resource monitor may be created to monitor the health of the application and to run recovery commands on special conditions.

Performance Toolbox Parallel Extensions for AIX: IBM Performance Toolbox Parallel Extensions for AIX (PTPE) collects and provides performance data for SP hardware and software. It is designed as an enhancement to Performance Toolbox for AIX, the preferred performance monitor for AIX systems. PTPE gives Performance Toolbox access to SP hardware and software statistics, and makes Performance Toolbox easier to use when monitoring a large number of systems. All this is done while retaining the same familiar interfaces to the performance data that you have come to expect from Performance Toolbox for AIX.

For information on PTPE, refer to *Performance Toolbox Parallel Extensions for AIX Guide and Reference*, SC23-3997.

Event Management and Group Services: Event Management provides comprehensive event detection by monitoring various hardware and software resources. Through Event Management, a client subsystem can be informed of events affecting its own resources, or of general system conditions that require attention by the subsystem. For information on Event Management, refer to *PSSP Event Management Programming Guide and Reference*.

Group services provides a general purpose facility for coordinating and monitoring changes to the state of a subsystem on a set of nodes. Group Services help both in the design and implementation of fault-tolerant subsystems, and in the consistent recovery of multiple subsystems.

IBM Virtual Shared Disk Usability Enhancements: A number of usability enhancements have been made to the IBM Virtual Shared Disk function of PSSP. Some of these include one command line to define and one command line to undefine VSDs, a graphical depiction of VSDs via Perspectives, and the ability to configure a subset of VSDs within a system partition.

IBM Recoverable VirtualShared Disk - Separate IBM Licensed Program Product: IBM Recoverable Virtual Shared Disk provides recovery for the VSDs with the help of user-level daemons that provide node UP/DOWN information and drive scripts tailored to enable VSDs to recover. The underlying physical disks must be physically twin-tail attached to both the primary and secondary nodes. RVSD also provides recovery services via daemons and an application programming interface. By utilizing these services, an application, such as a data base system, can now provide transparent recovery from a node failure. For more information on these and other enhancements made to the VSD and RVSD, refer to *RS/6000 Scalable POWERparallel Systems Managing Shared Disks: IBM Virtual Shared Disks, Data Striping Devices, and the IBM Recoverable Virtual Shared Disk Licensed Program* , SC23-3849.

SMIT Interface for Microcode Download Process: 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:

- Frame Twin-Tail
- 604 high node node
- SP Switch

Enter the SMIT fastpath command **smit supervisor** and use the Help Key (F1) for more information.

Extended Migration Support: For more information, refer to the white paper titled *Implementing Coexistence with PSSP 2.2* available in:

`http://www.rs6000.ibm.com/tech/`

Installing Your SP System

Installation involves these major steps:

1. Prepare and install or migrate the control workstation.
2. Enter node and 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.

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 and configuring the RS/6000 SP Ethernet connections on your control workstation. Other steps include verifying name resolution, installing IBM Parallel System Support Programs for AIX (PSSP) software, and configuring the SP authentication services.

Enter Node and Configuration Information

After the control workstation has been prepared, you can begin configuring the RS/6000 SP 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 *System Planning Guide* and understand the information presented there before you begin installing your system. (Both configuration methods are described throughout the detailed installation information, Chapter 2, “Installing and Configuring a New RS/6000 SP System” on page 13.)

After you enter all the configuration information, you press the PSSP System Monitor netboot button or the equivalent Perspectives button to network boot (netboot) the nodes to install and customize them. PSSP uses the information in the SDR to do the installation and customization.

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. PSSP 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 Reference Guide.

Network Installation

To install SP nodes, netboot the nodes to boot them over the network. Boot/Install Servers on the same network respond by installing the AIX image on the nodes. For more details, turn to “Install SP on the Nodes (Internals)” on page 5 and “Detailed Overview of Network Installation of a Node” on page 9.

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

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 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 recommends you use **script.cust** to complete your installation and **tuning.cust** to set initial network performance values. See Appendix C, “Sample script.cust File” on page 197 and Appendix D, “Sample tuning.cust File” on page 203 for printed samples.

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 4.1 image already on the node.

Boot Processing

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

Install SP on the Nodes (Internals)

Note: The information in this section is optional reading. Read on if you are interested in learning what is happening “under the hood” during SP installation.

AIX 4.1 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 *AIX Network Installation Management Guide and Reference*.

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

What Is a 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 an AIX 4.1 system or later with the NIM master file sets installed. A NIM master manages the configuration database containing the information for the NIM clients.

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.

Defining NIM Masters

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 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.

What Is a NIM Client?

A NIM client is a system installed and managed by a NIM master. SP supports the standalone type of NIM client. Nodes are defined as standalone clients for normal operations.

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 first node in each frame (or another node you specified as a NIM master) installs the other nodes. (The default is the first node in each frame.)

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

1. Installs the AIX 4.1 **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 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

Migrating Nodes

If you have a node currently running AIX 3.2.5, you can now migrate this node to AIX 4.1. This will migrate AIX on the node, all the LPPs that have filesets in the lppsource directory, and PSSP. To set a node to migrate:

- The node to migrate must have an AIX 4.1 boot/install server and the server must be running PSSP 2.2. To change the boot/install server, use the **spbootins -n** option.
- Change the **lppsource_name** of the node using SMIT. Set the **lppsource_name** to a 4.1 lppsource.
- Change the **code_version** of the node using SMIT to an appropriate level of PSSP.
- Run the **spbootins -r** command to set the node to migrate.
- Network boot the node

The result is that AIX will migrate from 3.2 to 4.1, the LPPs that have filesets in the lppsource directory will migrate, and PSSP will migrate to the correct PSSP level.

Storing NIM Information

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.

Machine objects represent the machine configuration for a NIM client. Each machine object contains attributes defining 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

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:

Resource Name	Description
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

Note: These are only examples of the resource objects. 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.

Working With the Basic AIX Image

The **spimg** installp image contains a **mksysb** or multiple **mksysb**s of an AIX 4.1 system you can use to install AIX 4.1 on the nodes in your RS/6000 SP system after you have successfully installed and configured your control workstation.

The **mksysb** is an image of a *minimal* AIX 4.1 system. This minimal system is made up of the following:

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

IBM provides the image as a base for getting your RS/6000 SP system up and running quickly. You can customize this image to meet the needs of your production environment. For instructions on customizing the minimal image, turn to "Task D. Power On and Install the Nodes" on page 63.

See the *Memo to Licensees* and **spimg lpp.README** for details of the contents of AIX 4.1.

Building a New AIX 4.1 Image

When you are installing your RS/6000 SP 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 this image on a node after you have installed the node using the basic image and additional LPPs.
- Use a standalone workstation (either the control workstation or a different standalone workstation).

  Note: After you have completed "Step 20: Initialize RS/6000 SP Authentication Services" on page 30, 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 this machine.

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. 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.

If you are generating your **mksysb** from a node, you can first use the basic image to install AIX 4.1 and PSSP LPP options on the node. Do not use a boot/install server node to generate the **mksysb**. Then you can use **script.cust** to install

additional LPPs and service your system requires. See Chapter 6, “Performing Software Maintenance” on page 183 for more details.

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** option.

After the image is created, you must copy it to /**spdata**/**sys1**/**install**/**images** on the control workstation or on the boot/install node. 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 Attribute in the SDR

After a new image has been created and copied to the control workstation, you are ready to update the SDR with the name of the new image for the nodes you want to reinstall. To define a new mksysb install image to be used for a node in the SDR, you can use the **spbootins** command or the SMIT server_dialog interface to do the following:

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

Detailed Overview of Network Installation of a Node

Note: 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)” on page 4.

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 or 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 and NIM performs the installation of the mksysb image. After the **mksysb** installation is complete, NIM invokes the **pssp_script** script resource.

Customization for Network Install

pssp_script transfers netinstall information files /**tftpboot**/*node_name***.install_info** and /**tftpboot**/*node_name***.config_info** from the boot/install server to the node and then performs the netinstall. **install_info** and **config_info** are used during a network installation of an AIX image. These files contain information necessary to successfully complete the netinstall.

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

- Client en0 IP address and host name
- Netinstall server IP address and host name
- Control workstation IP information and host name

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

- Node number
- Initial host name
- Default route
- 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)
  - bnc_select (DIX/BNC for Ethernet)

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 customize the SP 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.

ssp.basic, **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 (See “Step 23: Enter Site Environment Information” on page 41 in Chapter 2, Installing and Configuring a New RS/6000 SP System.) 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 disk. The node is then shut down and rebooted. During the subsequent boot, 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 option is performed now.

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 defined nodes.
- Configures the server as a NIM master
- Defines the following NIM resources:
  - spot
  - mksysb
  - script
  - lppsource

  - bosinst
- 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)
- Creates required authentication files, /**tftpboot**/*host name***-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.

Before You Begin

- 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 Chapter 4, “Migrating to the Latest Level of PSSP” on page 109.
- Make sure you have your configuration worksheets filled in 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 *System Planning Guide* 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 both methods are given. Use default options unless instructed to do otherwise.

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 System Planning Guide.

Finding Related Installation Information

You can find more information about SMIT in *IBM General Concepts and Procedures for RISC System/6000*.

You can find more information about the AIX 4.1 Network Installation Management in *AIX Network Installation Management Guide and Reference*.

The **installp** command is explained in *IBM AIX for RISC System/6000 Commands Reference*.

© Copyright IBM Corp. 1996

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 RS/6000 SP commands in this chapter are in **/usr/lpp/ssp/bin**, except where indicated.

To avoid entering the complete path name each time you want to invoke a RS/6000 SP command, add **/usr/lpp/ssp/bin** to the root user path in root's **.profile** file.

The RS/6000 SP authentication services **klist** command is in **/usr/lpp/ssp/kerberos/bin**. Add this path to root's **.profile** file.

The following is an example of the root user path statement in **.profile**:

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

In order to 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 Current Licensees*, 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 4.1.4 or later Base Operating System
   - TCP/IP
   - NFS
   - IBM Performance Aide for AIX Version 4.1 (perfagent.server)

     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.
3. The control workstation requires one serial port available per frame for the RS-232 cable that supports hardware monitoring and control. If your RS/6000 SP 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 *System Planning Guide* for detailed information about space requirements.

Notes:

a. 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 4.1 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 an 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.

b. All names and addresses of all IP interfaces on SP nodes must be resolvable on the control workstation before you install and configure the RS/6000 SP.

c. 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 RS/6000 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 RS/6000 SP System frames to the control workstation according to your RS/6000 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 RS/6000 SP 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.

Use SMIT or the **mkdev** command to define the RS-232 interfaces as they appear on your Control Workstation Worksheet.

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`

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

Step 6: 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 4.1 (except for built-in Ethernet adapters) set the transmit queue size to 160. The built-in Ethernet adapters can be set to 150. The FDDI adapter queue limit should be set to 250.

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`**
Note: You must reboot the control workstation in order for the changes to take effect.	

Step 7: Configure Ethernet Adapters

Use SMIT or the **chdev** command to configure each Ethernet adapter connecting your RS/6000 SP 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 accessed through the **info** command.

Refer to your RS/6000 SP Control Workstation Worksheet in the *System Planning Guide* for the IP addresses and netmask values of your Ethernet adapters.

Note: If 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 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 response. If you do not receive a response, reconfigure the adapter.

For example:

ping 129.33.34.1 -c 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 System Resource Controller daemon is not active`, then SRC is not running.

   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 root Maximum Default Processes

When you first install your RS/6000 SP system, the number of processes the non-root user can have is set to **40**, an AIX 4.1 default. You will not be able to continue installing your system with this default value—you must increase the number. You can do this using SMIT or the command line.

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 Tunables and Tunable Values

When you first install your RS/6000 SP system, the network tunable values are set to AIX 4.1 defaults. (A **tunable** is a SP 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 *Commands and Technical Reference*.

When you install PSSP on your control workstation, change the network tunables on the control workstation interface to the values in Table 1.

Table 1. Control Workstation Tunables

Tunable	Recommended 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:

```
/usr/sbin/no -a
```

AIX responds similarly to the following:

```
                thewall = 16384
                 sb_max = 163840
        net_malloc_police = 0
                 rto_low = 1
                rto_high = 64
               rto_limit = 7
              rto_length = 13
             arptab_bsiz = 7
               arptab_nb = 25
              tcp_ndebug = 100
                  ifsize = 8
          subnetsarelocal = 1
                   maxttl = 255
                ipfragttl = 60
          ipsendredirects = 1
             ipforwarding = 1
                  udp_ttl = 30
                  tcp_ttl = 60
               arpt_killc = 20
            tcp_sendspace = 65536
            tcp_recvspace = 65536
            udp_sendspace = 32768
            udp_recvspace = 65536
           rfc1122addrchk = 0
           nonlocsrcroute = 0
            tcp_keepintvl = 150
             tcp_keepidle = 14400
                bcastping = 0
                 udpcksum = 1
              tcp_mssdflt = 1448
          icmpaddressmask = 0
             tcp_keepinit = 150
ie5_old_multicast_mapping = 0
                  rfc1323 = 1
                ipqmaxlen = 100
       directed_broadcast = 1
              ipforwarding = 1
          subnetsarelocal = 1
```

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

```
/usr/sbin/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**. Note that this file is not created until after you install PSSP.

Step 12: Define Space for NIM Boot Images

Before creating an AIX 4.1 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 13: Define Space for the /spdata Directory

The /**spdata** directory contains **mksysb** and **installp** file sets. IBM recommends 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 *System Planning Guide* 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" 2. Do "Step 13.2: Create the File System for spdata" on page 22 3. Do "Step 13.3: Mount the /spdata File System" on page 22 4. 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 File System for spdata" on page 22 2. Do "Step 13.3: Mount the /spdata File System" on page 22 3. 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 13.4: 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 then using the default volume group **rootvg**.

You need to section off space on the control workstation disk, and this is one way to do it. IBM recommends you create a separate file system because of the large amount of SP data.

Note: You cannot create a separate volume group if: all control workstation disks are in use or the control workstation has only one physical volume.

To create a volume group, you can use SMIT or the command **mkvg**.

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. **/usr/sbin/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. **/usr/sbin/varyonvg spdatavg**

Step 13.2: 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**. You can use SMIT or the AIX command **crfs** to create the /**spdata** file system.

If using:	Do this:
SMIT	**TYPE** **smit crfs** **SELECT** Add a Journaled File System on a Previously Defined Logical Volume **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. **/usr/sbin/crfs -v jfs -d spdata_lv -m /spdata -A yes -p rw -t no**

Step 13.3: 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.

/usr/sbin/mount /spdata

Step 13.4: Expand an Existing File System

IBM does not recommend 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 AIX 4.1 LPP file sets, AIX **mksysb** images, and RS/6000 SP installp file sets.

You can use SMIT or the AIX command **chfs** to expand the root file system.

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. `/usr/sbin/chfs -a size=+781250 /`

Step 14: Create Required /spdata Directories

Note: Make sure you mount the new /**spdata** file system before you create the /**spdata** directories.

The RS/6000 SP requires you create sub-directories on the /**spdata** file system for storing critical PSSP data. 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 /spdata/sys1
/spdata/sys1/install	Main directory for PSSP installation	mkdir /spdata/sys1/install
/spdata/sys1/install/<name>/lppsource	Location of required AIX 4.1 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 RS/6000 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

Note:

<name> is the new lpp_source name for the nodes (such as aix414 if that is what you called the subdirectory with the AIX 4.1.4 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. you do not provide a name, setup_server assumes the value is *default*.

default is the default.

<code_version> is the version of code of the form PSSP-x.y. (such as, PSSP-2.2)

Make sure the directories have the permissions `rwxr-sr-x`.

Step 15: Copy the AIX 4.1 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.info.*
bos.net.*
bos.powermgt.*
bos.sysmgt.*
bos.terminfo.*
devices.*
X11.apps.*
X11.base.*
X11.compat.*
bos.rte.up.*
bos.rte.mp.*
bos.diag.*
X11.Dt.*
X11.fnt.*
X11.loc.*
X11.motif.*
X11.msg.*
X11.vsm.*
xlC.rte.*

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**.

You also must copy the IBM Performance Toolbox for AIX, Performance Aide (product number 5765-654) onto the control workstation from a separate media. This file set is called **perfagent.server** and must be in the lppsource directory.

1. Make sure you 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 *System Planning Guide* 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 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.
Command Line	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`
Note: 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.mte	Contains the magnetic tape extension

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.
Command Line	This example shows the product media on **rmt0**. Enter **`bffcreate -d /dev/rmt0 -t /spdata/sys1/install/pssplpp/<code_version> -X all`**

Note:

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.2.2.0.0** in **/spdata/sys1/install/pssplpp/**<**code_version**> to **pssp.installp**.

   a. Enter the following:

```
cd /spdata/sys1/install/pssplpp/<code_version>
mv ssp.usr.2.2.0.0 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/<name>
/usr/sbin/inutoc .
```

Step 17: Install a Basic AIX (mksysb) Image

Before You Begin

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. You can accomplish this by referring to "Customization" on page 5. 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 RS/6000 SP hardware contains the **spimg** installp image which is one or more **mksysb** images of the minimal AIX 4.1 system. You can use SMIT or **installp** to install the AIX 4.1 image directly from installation media to **/spdata/sys1/install/images/bos.obj.ssp.41**

If you intend to use your own **mksysb** image, copy it to **/spdata/sys1/install/images/bos.obj.ssp.41** 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. Whether you do a full installation or a minimal installation, all of the file sets selected are installed on the control workstation. 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 for Full and Minimal Installation

File set	Installed on the node	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 RS/6000 SP, including • SP System Monitor • SDR • Centralized Management Interface (CMI—the SMIT panels) • Installation and Configuration Commands
ssp.sysman		RS/6000 SP Management Tools including • User Management Support • Print Support • File Collections • Accounting Support • NTP
ssp.css		Device Drivers and Switch Support
ssp.jm		Resource manager for parallel application scheduling
ssp.public		Tar files for Amd, PERL, SUP, NTP, Tcl, TclX, TK-X11, and Expect.
ssp.gui (1)	Yes	SP System Monitor GUI and Perspectives
ssp.docs		Man Pages and Online Information
ssp.sysctl	Yes	The Sysctl component
ssp.authent		Authentication Server
ssp.top		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.
ssp.perlpkg		Perl4 and Perl5
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 System Planning Guide.
ssp.hacws		High Availibility Control Workstation Support
ptpe.program		PTPE program
ptpe.gui		PTPE graphical user interface
ptpe.docs		Man pages and InfoExplorer files
spimg		Contains a single file containing a **mksysb** image of a minimal AIX 4.1 system.

Note:

(1) ssp.gui is required on the control workstation for the System Monitor GUI and can optionally be installed on the node to use Perspectives.

(2) To determine which file sets are installed on individual nodes, issue the AIX **lslpp** command from the node.

Notes:

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

   You must install **ssp.authent** if you are using the RS/6000 SP 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 RS/6000 SP authentication facilities, you must first remove the other authentication service.

2. **ssp.clients** contains authentication commands and authenticated client services for the RS/6000 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. **ssp.clients** is required to perform system management tasks using SP System Monitor commands, AIX remote commands, or the sysctl remote command execution facility.

3. If you select any RS/6000 SP Management Tools from the **ssp.sysman** option, all tools on that option are automatically installed. See the RS/6000 SP Site Environment Worksheet in the *System Planning Guide*.

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

Installation without AIX Preinstalled

Because your system may not have AIX 4.1 preinstalled on the nodes, you should add an install image to your list of installation options. You can install **spimg**, AIX 4.1 (**bos.obj.ssp.41**) shipped with the RS/6000 SP PSSP package.

Or if you prefer, you can provide your own AIX image for installation on the nodes. See “Build an Installation Image” on page 186 for more information.

PSSP Installation Instructions

You can install PSSP using SMIT or the **installp** command. Login to the control workstation as root and follow either 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 options. For example, to install **ssp.basic** and **ssp.sysctl**, enter:
	`installp -a -d /spdata/sys1/install/pssplpp/<code_version> -X ssp.basic ssp.sysctl`
	Note: In AIX 4.1, **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`

Step 19: Customize the script.cust and tuning.cust Files

Two script files are provided for adding additional PSSP installation options and tuning information following the node network install. This step runs the **script.cust** and **tuning.cust** files after AIX is loaded on the node and the required PSSP options are installed. These files contain options that, when activated, can tune the system to better fit your environment's needs.

IBM recommends that you modify the **script.cust** file to install additional PSSP options, as necessary. The **tuning.cust** file contains recommended IP system tuning parameters that you should also decide on including. Refer to the sample files listed in the appendix of this book and copy these samples from **/usr/lpp/ssp/samples** to **/tftpboot** before altering them.

Ensure that the permissions for these two files are set to 644 `rw-r--r--`.

Step 20: 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 System Planning Guide. See the *System Planning Guide* 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:

- Creates a primary authentication server and database

- Creates a secondary authentication server and database, after the primary server has been initialized
- Initializes the control workstation or other RISC System/6000 workstation to use AFS authentication
- 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 20.1: Initializing as the Primary Authentication Server"
Secondary Authentication Server	"Step 20.2: Initializing as a Secondary Authentication Server" on page 34
Authentication Client System	"Step 20.3: Initializing as an Authentication Client System" on page 36
Use AFS Authentication	"Step 20.4: Initializing to use AFS Authentication" on page 38
Note: Select only one authentication step to follow. Do not perform the steps for the authentication server you did not choose.	

Before You Begin

- <screenclear> shows where **setup_authent** clears the screen before displaying an explanation of the next part of the initialization procedure.
- *poobah* 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 the 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 20.1: Initializing as the Primary Authentication Server

This example shows the procedure you should follow 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
<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: poobah

Instance: admin

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


New Password: PoobahPassword
Verifying, please re-enter
New Password: PoobahPassword

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>
<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 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.
 ********************************************************************
Kerberos Initializion for "poobah.admin"
Password: PoobahPassword

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

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

Step 20.2: Initializing as a Secondary Authentication Server

Before You Begin

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

This example shows the procedure you should follow to initialize a secondary authentication server on the RS/6000 SP 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 when the primary server was set up. 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 RS/6000 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: poobah

Kerberos Initialization for "poobah.admin"

Password: PoobahPassword
backup.abc.com: success.


backup.abc.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:  poobah.admin@XYZ.ABC.COM

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

Step 20.3: Initializing as an Authentication Client System

Before You Begin

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

This example shows the procedure you should follow to initialize the RS/6000 SP 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.

   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. 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.

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
setup_authent: This system is not listed as a Kerberos server in /etc/krb.conf.
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: poobah

Kerberos Initialization for "poobah.admin"

Password: PoobahPassword

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

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

# <end_of_example>
```

Step 20.4: Initializing to use AFS Authentication

Before You Begin

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

This example shows the procedure you should follow 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 *System Planning 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/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 to use AFS authentication.

Note: The following message is always displayed 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:  poobah.admin@XYZ.ABC.COM

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

# <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 14, **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 Security Services, Obtaining Authentication Credentials". With AFS authentication, **kinit** will work properly after step 14 is completed.

Step 21: 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
- Brings up the Perspectives Launch Panel.
- 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
```

Step 22: Run SDR and System Monitor Verification Tests

This step directs you to run verification tests that check for correct installation of the SDR and the SP System Monitor. You can run these verification tests from SMIT panels or from the command line.

If using:	Do this:
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
Command Line	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 **SDR_test** and **spmon_itest** and on what these tests do.

See the section about Diagnosing RS/6000 SP Problems in the *Diagnosis and Messages Guide*.

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

This section describes the steps you take to enter the information defining the SP2 configuration. After you prepare the control workstation and install the PSSP software, you are ready to enter the data to define your SP2 configuration.

Step 23: Enter Site Environment Information

Before You Begin

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 SMIT or the **spsitenv** command to enter information about your site environment. The *System Planning Guide* contains a worksheet for these site environment values. Use the information in the *System Planning Guide* to fill out the worksheet before you enter this data.

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 *System Planning 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 or not you want to use Amd to automount user's home directories
- How you want RS/6000 SP Print Management integrated in your network
- 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.

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:
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 Δ 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/aix414/lppsource** for you installation configuration.
	`spsitenv cw_lppsource_name=aix414`

Step 24: Enter Frame Information and Reinitialize the SDR

This step creates frame objects in the SDR for each frame in your RS/6000 SP 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 RS/6000 SP frames using SMIT or the **spframe** command. See the *Commands and Technical Reference* for **spframe** syntax and parameter information.

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:
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**.) **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 25: Start System Partition-Sensitive Subsystems

The PSSP 2.2 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 Controller via the **syspar_ctrl** command. For a more complete description of partition-sensitive subsystems, refer to the section "Managing Partition-Sensitive Subsystems" in the *Administration Guide*.

To add and start the partition-sensitive subsystems, issue the **syspar_ctrl -A** command.

Note: If you are performing a migration install and your system contains more than one system partition, use the **-G** flag with the **syspar_ctrl** command. Issue the **syspar_ctrl -A -G** command to add and start the subsystem in each system partition.

Step 26: Verify System Partition-Sensitive Subsystems Have Started

To view a complete list of the subsystems managed by the Syspar Controller, issue the **syspar_ctrl -E** command.

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

Filtering out subsystems whose status you are interested, 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 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, first try to stop and delete all of the partition-sensitive subsystems, issue the command:

syspar_ctrl -D.

Then try to again add and start all of the partition-sensitive subsystems by executing the following command:

syspar_ctrl -A.

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

Step 27: Verify System Monitor Installation

Perform this step to verify that the SP System Monitor and Perspectives have been correctly installed. You can run these verification tests from SMIT panels or from the command line.

If using:	Do this:
System Monitor GUI	**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 28: 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:
System Monitor GUI	From the System Monitor pop-up window: **SELECT** SP **SELECT** All Node Summary Display Δ The selection screen for node variables appears. **SELECT** 3DigitDisplay from the list of variables **PRESS** Display all-node summary Δ The 3-Digit Display Summary appears.
Perspectives	**SELECT** the Hardware icon by double clicking ▲ The Hardware Perspectives menu appears with the Nodes Pane showing by default. The number of frames and assignment of nodes within the frames should match your configuration.
spmon	Type: `spmon -d`

You should see the frames represented with thin, wide, or 604 high node LED displays, 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.

Step 29: Update the State of the Supervisor Microcode

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

- You have just performed “Step 21: 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 Chapter 5, “Reconfiguring the RS/6000 SP System” on page 149. 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 Chapter 6, “Performing Software Maintenance” on page 183 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.

You can use either SMIT or the command line to perform this task.

<table>
<tr><th>If using:</th><th colspan="2">Do this:</th></tr>
<tr><td>SMIT</td><td colspan="2">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:
• Frame Twin-Tail
• 604 high node node
• SP Switch
Enter the SMIT fastpath command smit supervisor and use the Help Key (F1) for more information.</td></tr>
<tr><td></td><td>To update:</td><td>Do this:</td></tr>
<tr><td></td><td>All the supervisors</td><td>SELECT Update *All* Supervisors That Require Action</td></tr>
<tr><td></td><td>A subset of supervisors</td><td>SELECT Update Selectable Supervisors That Require Action</td></tr>
<tr><td>Command line</td><td colspan="2">Issue the spsvrmgr command. Refer to the Commands and Technical Reference for more information.</td></tr>
</table>

Step 30: Enter Required Node Information

Before You Begin

- 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 *System Planning 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 configuration mechanisms after the nodes are powered on.

Enter information about your RS/6000 SP nodes attached to each Ethernet adapter using SMIT or the **spethernt** command.

Note that you can access SMIT using Perspectives as well by typing **perspectives** to bring up the Perspectives Launch Pad and then selecting **smit config_data** from the Launch Pad. The SP Configuration Data Base Management menu appears. Select Enter Data Base Information. The Enter Data Base Information menu appears. Select Node Data Base Information. The Node Data Base Information menu appears. Select SP Ethernet Information. From this point, you can follow the rest of the SMIT steps described in the following table.

If you want to use the **spethernt** command, but want more information about command syntax and parameters, see the *Commands and Technical Reference* for syntax and parameter information.

If using:	Do this:
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 RS/6000 SP 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 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 **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.

Note:

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**

spethernt	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 dix** 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 dix -s no 1 1 16 129.33.32.1 255.255.255.192 129.33.32.200**

Step 31: Acquire Hardware Ethernet Addresses

Before You Begin

- Do not do this step on a 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 adapter for you. (This makes **sphrdwrad** take longer to run.)

To write the hardware Ethernet addresses to the SDR, use SMIT or issue the **sphrdwrad** command.

If using:	Do this:
Perspectives	**SELECT** smit config_data from the Launch Pad. Δ The SP Configuration Data Base Management menu appears. **SELECT** Enter Data Base Information Δ The Enter Data Base Information menu appears. **SELECT** Node Data Base Information Δ The Node Data Base Information menu appears. **SELECT** SP Ethernet 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** 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.
Note: If this scenario fails, look for the node conditioning instructions in the *Diagnosis and Messages Guide*.	

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`

See the *Commands and Technical Reference* for **sphrdwrad** syntax and parameter information.

Step 32: Verify Ethernet Addresses Were Acquired

Use SMIT, Perspectives, or issue the **splstdata** command.

If using:	Do this:
Perspectives	**SELECT** smit config_data from the Launch Pad Δ The SP Configuration Data Base Management menu appears. **SELECT** List Data Base Information Δ The List Data Base 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 Boot/Install Information ▲ The List Node Boot/Install Information window appears. **TYPE** The Start Frame, Start Slot, and Node Count *or* Node List **PRESS** **Do**.
splstdata	**Warning:** 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 -b`

Step 33: Configure Additional Adapters for Nodes

Before You Begin

This step is optional if your frame does not have a switch or does not require other 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 *System Planning 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.

Note: 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. See the *Commands and Technical Reference* for **spadaptrs** syntax and parameter information. The *System Planning Guide* contains additional information on IP addressing for the switch.

If using Perspectives. access **smit config_data** from the Launch Pad. The SP Configuration Data Base Management menu appears. Select Enter Data Base Information. The Enter Data Base Information menu appears. Select Node Data Base Information. The Node Data Base Information menu appears. Select SP Ethernet 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 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.
	Note: `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?

Note:

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. **Note:** 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
- You want to set up alternate default routes or netmasks for certain IP address ranges

If using:	Do this:

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.
	Note: `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.)
	Note: These fields are used only for the **css0** adapter:
	• Skip IP Addresses for Unused Slots?
	• Enable ARP for the css0 Adapter?
	• Use Switch Node Numbers for css0 IP Addresses?

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 34: Configure Initial Host Names for Nodes

Before You Begin

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 host name 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 see 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 host names to be used, as well as whether the long or short form should be used. See the *Commands and Technical Reference* for more information.

Use SMIT, Perspectives, or issue the **sphostnam** command. See the *Commands and Technical Reference* for **sphostnam** syntax and parameter information.

If using:	Do this:
Perspectives	**SELECT** **smit config_data** from the Launch Pad. ▲ The SP Configuration Data Base Management menu appears. **SELECT** Enter Data Base Information Δ The Enter Data Base Information menu appears **SELECT** Node Data Base Information Δ The Node Data Base Information menu appears **SELECT** SP Ethernet 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 35: Set Up Nodes to Be Installed

Before You Begin

- Do this step if you want to change the default installation settings for all 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 38: 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 you have exported any directories below /**usr**, 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.

This step does the following:

- Changes the default boot/install information in 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 boot/install server
- You have multiple frames 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
- The name of the installation image you are using if you do not want to use the default image, **bos.obj.ssp.41**

If you want different nodes to be installed by a different boot/install server, you must specify which nodes they are and which node will install them.

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. This specifies a disk in a specific hardware location:

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

You can specify multiple hardware locations, separated by colons, as follows:

```
00-00-00-0,0:00-00-00-1,0
```

Note: 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 recommends using the hardware location format.

Use SMIT, Perspectives, or issue the **spbootins** command. Refer to the *Commands and Technical Reference* for **spbootins** syntax and parameter information.

If using:	Do this:
Perspectives	**SELECT** **smit config_data** from the Launch Pad. Δ The SP Configuration Data Base Management menu appears. **SELECT** Enter Data Base Information Δ The Enter Data Base Information menu appears **SELECT** Node Data Base Information Δ The Node Data Base Information menu appears **SELECT** SP Ethernet Information From this point, you can follow the rest of the SMIT steps described in the following table.
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 **hdisk1** and **hdisk2** as alternate installation disks for nodes 10 through 16: **spbootins -s no -h hdisk1,hdisk2 1 10 7** If you are issuing the **spbootins** command for the last time in this installation, have it run **setup_server** (the **-s yes** flag). For example: **spbootins -s yes -h hdisk1,hdisk2 1 10 7** 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 aix414 for nodes 1 through 16 . **spbootins -s no -v aix414 1 1 16** If you need to change the PSSP code_version level from PSSP-2.1 to PSSP-2.2 on nodes 17,18,21,22 , you may execute **spbootins -s no -p PSSP-2.2 -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: Note that hdisk0 is the default.	

Step 36: Verify All Node Information

Use SMIT or issue the **splstdata** command. See the *Commands and Technical Reference* for **splstdata** syntax and parameter information.

<table>
<tr><th>If using:</th><th colspan="2">Do this:</th></tr>
<tr><td>SMIT</td><td colspan="2">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 24: Enter Frame Information and Reinitialize the SDR” on page 42
Node data — “Step 30: Enter Required Node Information” on page 47
Additional adapters — “Step 33: Configure Additional Adapters for Nodes” on page 51
TYPE smit list_data
▲ The List Database Information Window appears.
SELECT Each panel listed. Verify all information is correct.
PRESS Done to exit SMIT.</td></tr>
<tr><td rowspan="6">splstdata</td><td>To display SDR:</td><td>Enter:</td></tr>
<tr><td>Site environment data</td><td>splstdata -e</td></tr>
<tr><td>Frame data</td><td>splstdata -f</td></tr>
<tr><td>Node data</td><td>splstdata -n</td></tr>
<tr><td>Adapter data</td><td>splstdata -a</td></tr>
<tr><td>Boot/install data</td><td>splstdata -b</td></tr>
<tr><td colspan="3">Note: 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.</td></tr>
</table>

Changing the Default Network Tunable Values

At this point, you can change the default network option tunable values that are set when a node is installed or booted. Changing the tunable values from the AIX 4.1 default values improves the performance of the networks and switch on the RS/6000 SP. This mechanism preserves changes to the network tunable values across boots of the nodes.

The following steps enable you to load a set of network tunable values onto the nodes when they are installed. These values are copied to each node from the control workstation during installation or customization.

1. On the control workstation, copy the file **/usr/lpp/ssp/samples/tuning.cust** to **/tftpboot/tuning.cust**.
2. Select the tunable values that are best for your system. Refer to Table 3 on page 61 and Table 4 on page 61 for recommended values based on the adapters installed on the nodes.
3. Edit the **tuning.cust** file by uncommenting the **/usr/sbin/no** commands and changing the default tunable values.

Table 3. Initial Values for AIX 4.1 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

Note: *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 recommended settings in Table 4.

Table 4. Initial Values for Other AIX 4.1 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
tcp_mssdflt	4044	4300	4128

Modifying Tunables

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 *SP 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.

Step 37: Configure Control Workstation as Boot/Install Server

Before You Begin

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):

- Amd
- File Collections
- NTP
- Print Service
- 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 recommended 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, "Boot/Install Server Configuration Commands" on page 209.

If using:	**Do this:**
Perspectives	**SELECT** **smit config_data** from the Launch Pad. Δ The SP Configuration Data Base Management menu appears. **SELECT** Enter Data Base Information Δ The Enter Data Base Information menu appears. **SELECT** Run setup_server command
SMIT	**TYPE** **smit enter_data** ▲ The Enter Database Information window appears. **SELECT** Run setup_server Command
Command Line	Enter: `setup_server` with no parameters.
Note: 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. Power On and Install the Nodes

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

Step 38: 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 or AFS
- Configuring adapters that are not configured automatically
- Changing system tunable values

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 4.1 nodes. See Appendix C, “Sample script.cust File” on page 197 for a sample **script.cust** file. 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 39: 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. You can run this verification test from SMIT panels or from the command line.

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

Step 40: Set Up the Switch

Before You Begin

If you plan to do "Step 43: Set Up System Partitions" on page 69, skip the following steps:

- Step 40: Set Up the Switch
- Step 41: Verify the Switch Primary and Primary Backup Nodes

and go directly to "Step 42: Set Switch Clock Source for All Switches" on page 68.

If you do not have a switch., go to "Step 44: Network Boot Optional Boot/Install Servers" on page 70.

The optional switch connects all the nodes in the RS/6000 SP 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 have the switch. You create this file by copying one of the default topology files provided for each RS/6000 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.

Step 40.1: 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.*NSBnum***nsb.***ISBnum***isb**.*type*

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 *System Planning Guide*.

Step 40.2: 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. Therfore, if you are using an **expected.top** bypass file, ensure that it is removed from all nodes when it is no longer needed.
2. The first **Estart** on the SP Switch can take longer depending upon your configuration.

Step 40.3: 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 Cluster_Mgmt icon Δ 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** 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` See the *SP Commands and Technical Reference* for more information on **Eannotator**.

Step 40.4: Storing the Switch Topology File in the SDR

Before You Begin

If you entered **Eannotator -O yes** or **yes** on the Topology File Annotator menu in "Step 40.3: Annotating a Switch Topology File" on page 66, skip this step.

If using:	Do this:
Perspectives	**SELECT** the Cluster_Mgmt icon Δ 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`
Note: See the *SP Commands and Technical Reference* for more information on **Etopology**.	

Step 41: Verify the Switch Primary and Primary Backup Nodes

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 new node type has been developed 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). Use SMIT or the **Eprimary** command to verify this node or change the primary to another node.

If using:	Do this:
Perspectives	**SELECT** the Cluster_Mgmt icon Δ 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** 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.

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

See the *Commands and Technical Reference* for command syntax.

Step 42: 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 *System Planning Guide* for the Eclock topology file names.

If using:	Do this:
Perspectives	**SELECT** the Cluster_Mgmt icon Δ 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. **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. See the *Commands and Technical Reference* for more information on the **Eclock** command. **Warning:** 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 43: Set Up System Partitions

This step is optional. The PSSP 2.2 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 44: Network Boot Optional Boot/Install Servers” on page 70.

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.

Note: You do not have to partition your system now as part of this installation. You can partition it later. Follow the procedure described in the *Administration Guide*.

Step 44: Network Boot Optional Boot/Install Servers

Before You Begin

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

Use the System Monitor GUI or Perspectives 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>
```

Note: Depending on the size of the image you are installing and the capacity of your RS/6000 SP Ethernet network, you should network boot (or reboot) eight nodes per boot/install server at a time.

If using:	Do this:
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. ▲ 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.
Perspectives	**SELECT** the Hardware icon by double clicking on it. **SELECT** the Nodes pane **SELECT** Actions → Nodes → 3-digit display Δ The 3 digit display appears. **SELECT** Nodes to be netbooted **SELECT** Actions → Nodes → Netboot **SELECT** Apply Δ 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.
Command Line	Type `nodecond frame_number node_number`

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 72 lists the sequence of LED values a node goes through. This 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 SP Ethernet
- How busy the network installation node is

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.
	Blank	
	570	Configuring virtual SCSI devices.

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

Time (min:sec)	LED Value	Description
	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.
22:30		
	Blank	
23:00		

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

Time (min:sec)	LED Value	Description
	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.
34:00		
	570	Configuring virtual SCSI devices.

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

Time (min:sec)	LED Value	Description
	538	The configuration manager is invoking a configuration method.
34:30	Blank	

Step 45: Verify that System Management Tools Were Correctly Installed on Boot/Install Servers

Before You Begin

Do this step for each boot/install server.

Now that the boot/install servers are powered up, run the verification test to check for correct installation of the System Management tools on these nodes. You can run this verification test from the control workstation to verify the boot/install servers using SMIT panels or the command line.

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 verification test fails.

Step 46: Network Boot the Remaining RS/6000 SP Nodes

Before You Begin

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

Repeat the procedure used in Step 44: Network Boot Optional Boot/Install Servers on page 70 to network boot and install, or customize the remaining RS/6000 SP nodes.

Note: 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 *System Planning 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 SP 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 Δ 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 47: Verify Node Installation

Before You Begin

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:
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
Perspectives	**SELECT** the hardware icon by double clicking on it. Δ The Hardware Perspectives appears. **SELECT** the Nodes Pane **SELECT** View → Monitor Δ The Set Monitoring for Nodes dialog box appears. **SELECT** the hostResponds condition **PRESS** Apply Δ 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 Δ The node icons will turn black. **SELECT** the powerLED condition in the Set Monitoring for Nodes dialog box. **PRESS** APPLY Δ The nodes should now be colored green.

Step 48: Run Verification Tests on All Nodes

Before You Begin

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. You can run these verification tests from SMIT panels, Perspectives, or from the command line.

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	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 49: Start the Optional Switch

Before You Begin

- 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.

This step initializes the switch. You can perform this step from SMIT panels or from the command line. You can also access the **smit switch_ops** using Perspectives.

If using:	Do this:
SMIT	**TYPE** **smit switch_ops** ▲ The Perform Switch Operations Menu appears. **SELECT** Start Switch
Estart	Enter: **Estart**

Step 50: Verify the Switch Was Installed Correctly

Before You Begin

- 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.
Command Line	Enter: `CSS_test`

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:
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*.
Perspectives	**SELECT** the Hardware icon by double clicking on it. **SELECT** the Nodes Pane Δ The Nodes Pane receives focus. **SELECT** View → Monitor Δ The Set Monitoring for Nodes dialog box appears. **SELECT** the switch_responds condition **PRESS** Apply Δ 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.

Step 51: 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 4.1 (except for built-in Ethernet adapters) set the transmit queue size to 160. The built-in Ethernet adapters can be set to 150. The FDDI adapter queue limit should be set to 250.

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 node 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=160`**
Note: You must reboot the node in order for the changes to take effect.	

Run Postinstallation 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* and the *System Planning 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 *Administration 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).

Read This!

The information in this chapter applies to feature 3936 of program number 5765-529. Check with your IBM representative to make sure this feature is available.

The information in this chapter is optional—you do not have to install HACWS in order to run your SP system. 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.)

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 & Facilities*, SC23-2767.

Before You Begin

Plan your HACWS installation. This will help make your installation more efficient and successful. For more information about planning for HACWS installation, see the *SP System Planning Guide*.

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 V4.2 on both control workstations.
- HACWS supports only a single backup control workstation.

© Copyright IBM Corp. 1996

- Resource Manager does not participate in HACWS. You must start it manually after a fail over or reintegration.
- 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.

Finding Related Installation Information

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

- *AIX HACMP/6000 Concepts & Facilities*, SC23-2767
- *AIX HACMP/6000 Planning Guide*, SC23-2768
- *AIX HACMP/6000 Installation Guide*, SC23-2769
- *AIX HACMP/6000 Administration Guide*, SC23-2770
- *System Planning Guide*, GC23-3902
- *Administration Guide*, SH26-2486
- *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*, SC23-2767
- *AIX HACMP/6000 Planning Guide*, SC23-2768
- *AIX HACMP/6000 Installation Guide*, SC23-2769
- *AIX HACMP/6000 Administration Guide*, SC23-2770
- *System Planning Guide*, GC23-3902
- *Administration Guide*, SH26-2486

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 *System Planning Guide*. Here, refer to the following diagrams that illustrate a high-level look at the High Availability Control Workstation

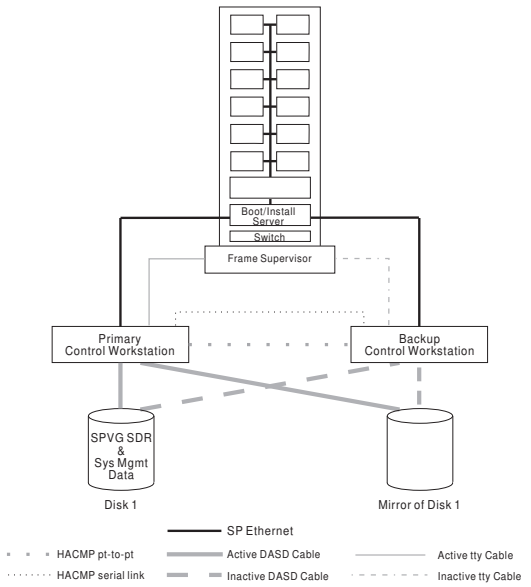

Figure 1. High Availability Control Workstation With Disk Mirroring

Sample Scenario: Setting Up a High Availability Control Workstation

Review the following example to understand how to set up your network configuration:

Assume that your system has a single control workstation named *dutchess.xyz.com* and it will serve as the primary control workstation after you install HACWS. The workstation you add will become the backup control workstation. The name of the backup control workstation is *ulster.xyz.com*.

The SP nodes get control workstation services by accessing the network interface whose name matches the hostname of the primary control workstation. In this example, the SP nodes get control workstation services by accessing *dutchess.xyz.com*. If the primary control workstation fails and the backup control workstation takes over, the backup control workstation assumes the network identity of *dutchess.xyz.com*.

The *dutchess.xyz.com* network interface gets configured on the control workstation currently providing the control workstation services. HACMP refers to *dutchess.xyz.com* as a service address (or service interface). The primary control workstation must use a different network address when it reboots in order to avoid a network address conflict between the two control workstations. HACMP refers to this alternate network address as a boot address (or boot interface). In this example, the boot address of the primary control workstation is *dutchess_bt.xyz.com*.

In addition, HACWS requires the backup control workstation to always be reachable via a network interface whose name matches its hostname. In this example, this name is *ulster.xyz.com*. This network interface does not get identified to HACMP. If you have no available adapter upon which to configure the *ulster.xyz.com* network interface, you can use an IP alias.

Each control workstation in this example configuration contains one ethernet adapter, connected to the SP Ethernet network. After the two control workstations are booted and before HACMP is started, their network configuration looks like the one illustrated in Figure 2.

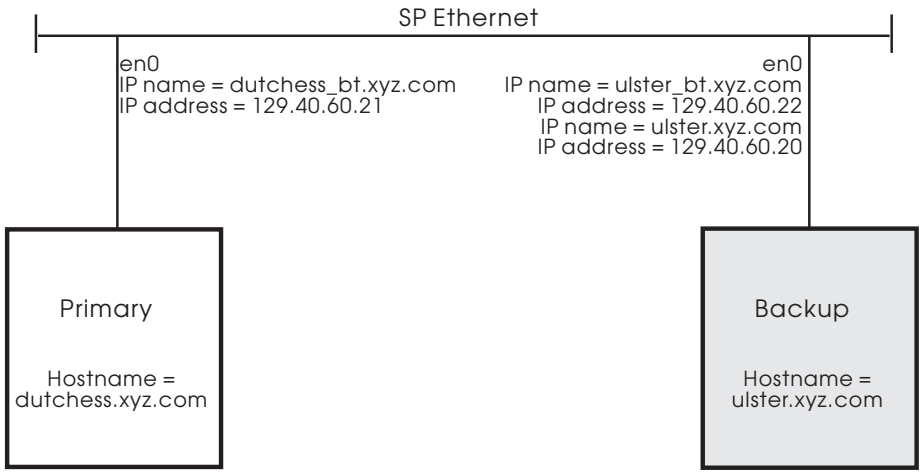

Figure 2. Initial control workstation Network Configuration

At this point, neither machine is providing control workstation services, so the *dutchess.xyz.com* network interface is not available. The ethernet adapter on the primary is configured with its boot address *dutchess_bt.xyz.com* and the ethernet adapter on the backup is configured with its boot address *ulster_bt.xyz.com*. Since there is only one network adapter, the network interface *ulster.xyz.com* must be configured as an IP alias on the backup control workstation.

Note: Both IP addresses 129.40.60.22 and 129.40.60.20 are assigned to the adapter **en0** on the backup control workstation. If another network adapter is available, you do not have to use an IP alias.

When the operator starts HACMP on both control workstations, the first control workstation to start HACMP becomes the active control workstation. (The operator selects the machine to become the active control workstation by starting HACMP on it first.) If HACMP is started first on the primary control workstation, then after HACMP is started on the backup control workstation, the control workstations look like the ones illustrated in Figure 3.

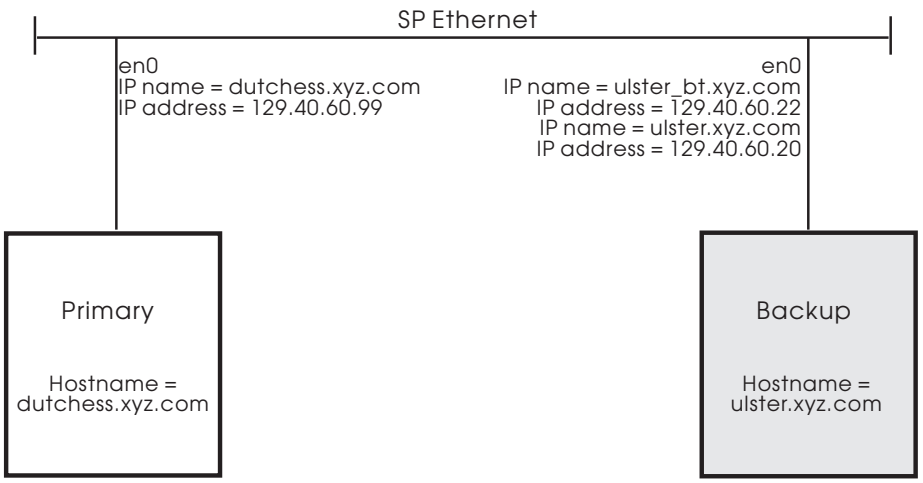

Figure 3. Starting HACMP

The only change to the network configuration is the boot address *dutchess_bt.xyz.com* on the primary control workstation has been replaced by the service address *dutchess.xyz.com*.

If the primary control workstation should fail and the backup control workstation take over, the control workstations look like the ones illustrated in Figure 4 on page 88.

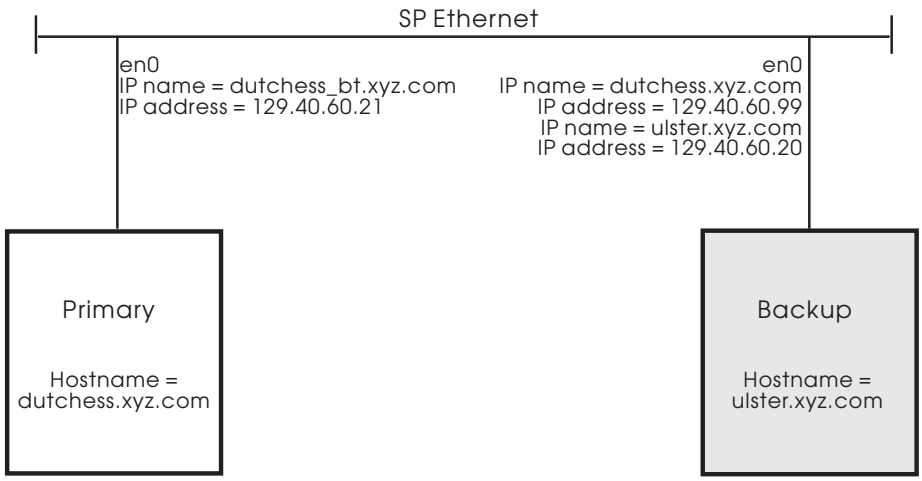

Figure 4. control workstation Failover

If the primary control workstation is still running, then its ethernet adapter is back on its boot address *dutchess_bt.xyz.com*, and the boot address *ulster_bt.xyz.com* on the backup control workstation has been replaced by the service address *dutchess.xyz.com*. The SP nodes continue to get control workstation services by accessing *dutchess.xyz.com*.

Note: The network interface *ulster.xyz.com* remains configured on the backup control workstation.

You can identify multiple network interfaces to move back and forth between the two control workstations along with the control workstation services. Some possible reasons for doing this are:

- You have an SP system with a large number of nodes and multiple ethernet adapters on the control workstation connected to the SP Ethernet network.
- You want the control workstation to provide a separate network interface for each SP system partition.
- You want a network interface on an external network to allow workstations outside of the SP system transparent access the active control workstation.

Each of these network interfaces is effectively a service address. However, the number of service addresses identified to HACMP cannot exceed the number of network adapters. Use IP address aliasing to make up the difference.

In this example, each control workstation has only one network adapter. Since *dutchess.xyz.com* is defined to HACMP as a service address, any additional "effective" service addresses must be configured using IP address aliases. If you added an SP system partition whose network interface name on the control workstation is *columbia.xyz.com* to this example configuration, it would look like Figure 5 on page 89 when the backup control workstation is active.

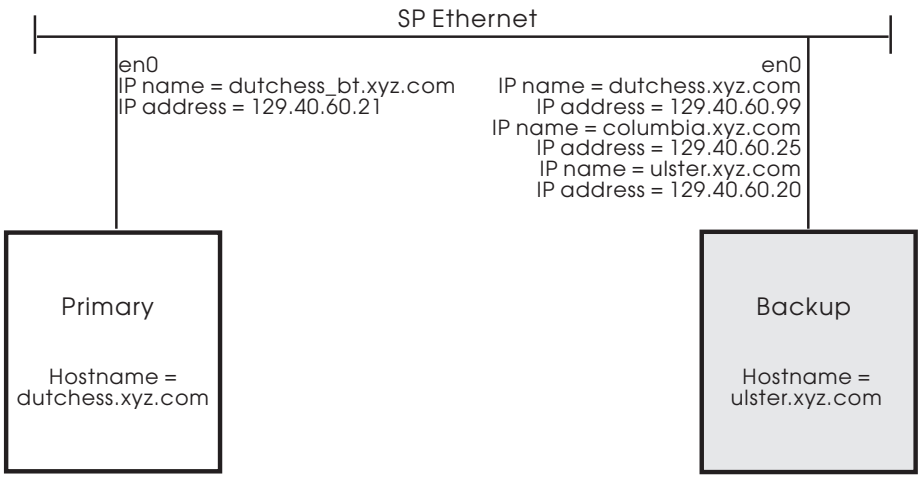

Figure 5. Multiple Network Interfaces

The HACMP service address *dutchess.xyz.com* is configured on adapter **en0** on the backup control workstation and the network interfaces *columbia.xyz.com* and *ulster.xyz.com* are configured on adapter **en0** as IP aliases. The service address *dutchess.xyz.com* is identified to HACMP. For each service address that is identified to HACMP, there must be boot addresses for both control workstations. The boot address *dutchess_bt.xyz.com* is identified to HACMP for the primary control workstation, and the boot address *ulster_bt.xyz.com* is identified to HACMP for the backup control workstation

At this point, if you have not done so already, you need to do the following:

1. Determine the control workstation service addresses for your configuration.
2. Determine which service addresses should be identified to HACMP and which service addresses need to be configured using IP aliases. The hostname of the primary control workstation (*dutchess.xyz.com*) must always be identified to HACMP as a service address. Remember the number of service addresses identified to HACMP cannot exceed the number of network adapters.
3. Determine the boot addresses for your configuration. The number of boot addresses on each control workstation will match the number of service addresses defined to HACMP. For example, if you identify three service addresses to HACMP, then you need to identify six boot addresses—three boot addresses on each control workstation.
4. Make sure the hostname of the backup control workstation (*ulster.xyz.com*) is always a valid network interface on the backup control workstation.
5. If your site uses a name server, make sure that all of these network interfaces have been added to your name server.

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 already be completely installed and operating correctly before installing High Availability Control Workstation.

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.

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 *Site Planning Guide* for instructions. The use of a serial network with HACMP is strongly recommended. 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 RS/6000 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.

Task B. Update RS/6000 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

To install PSSP on the backup control workstation, refer to the instructions in “Task B. Install PSSP on the Control Workstation” on page 26. Do not run any configuration commands. (Do not run **install_cw**.)

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 secondary 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>.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: poobah
Kerberos Initialization for "poobah.admin"
Password: PoobahPassword
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:  poobah.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 RS/6000 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
setup_authent: This system is not listed as a Kerberos server in /etc/krb.conf.
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: poobah
Kerberos Initialization for "poobah.admin"

Password: PoobahPassword
# klist
Ticket file:    /tmp/tkt0
Principal:  poobah.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. To accomplish this, enter the following commands on the backup control workstation:

```
/usr/lpp/ssp/rcmd/bin/rcp -p primary_name:/etc/krb-srvtab /etc/krb-srvtab.primary
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.

On the backup control workstation, run the **/usr/lpp/ssp/kerberos/bin/kadmin** command 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 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 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 85.) 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” on page 106.

Step 20: Migrate Internal File System

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

Before You Begin

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

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 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. Answer **no** to the `quorum required` question.
   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. Make sure quorum is disabled on the primary control workstation by using **smit chvg**. Answer **no** to the `quorum required` question.

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 104 sets I/O pacing to the HACMP recommended starting points. If you want to let **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 "Sample Scenario: Setting Up a High Availability Control Workstation" on page 86) 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 "Step 2: Plan Network Configuration" on page 85.

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 (see "Sample Scenario: Setting Up a High Availability Control Workstation" on page 86), 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 (see "Sample Scenario: Setting Up a High Availability Control Workstation" on page 86), 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 6. 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 7. 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 8. 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 8 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.
Command Line	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.
Command Line	Enter: `/usr/sbin/hacws/spcw_addevents`

If you want to further customize cluster event processing, follow the instructions in Chapter 5 of the *System Administration Guide*.

Step 30: Add IP Address Aliases

In "Step 2: Plan Network Configuration" on page 85 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 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 your favorite 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**.
Command Line	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**.
Command Line	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 "SPCW_APPS COMPLETE" /tmp/hacmp.out

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 106.

Cause a Failover

After cluster services have started on the primary control workstation, tell 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."

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 106.

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 "SPCW_APPS COMPLETE" /tmp/hacmp.out

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 2.2 and AIX 4.1.4 either from PSSP 1.2 and AIX 3.2.5 or from PSSP 2.1 and AIX 4.1.3 or AIX 4.1.4. Note that minimum PTF levels are recommended for both PSSP 1.2 and PSSP 2.1. For planning purposes, migration testing was performed at IBM with PSSP 1.2 at PTF tape 24 and PSSP 2.1 at PTF tape 16. Note the *Memo to Users* or consult the latest README file.

Preparing to Migrate

1. Read the Planning for Migration chapter in the *Planning Guide*. In addition, you should know the initial system configuration and which nodes will reside in each system partition. You must know which boot/install server nodes will service which AIX and PSSP levels and have worksheets that define the boot install information for each node that is being migrated to PSSP 2.2.
2. Ensure that your system has a minimum of 2 GB of space for the /**spdata** file system on the control workstation. If you will have any PSSP 1.2 nodes, ensure that your system has a PSSP 1.2 node that has enough space to provide boot/install services to other PSSP 1.2 nodes. To manage PSSP 1.2 nodes, you need at least two boot/install servers.
3. 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.
   - 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.

Steps to Migrate the Control Workstation from PSSP 1.2 to PSSP 2.2

Follow the steps in this section if you have chosen the **migration** approach to upgrading from PSSP 1.2 to PSSP 2.2 as described in the migration chapter of the *System Planning Guide*. Before doing these steps, quiesce all jobs and stop the Resource Manager on the RS/6000 SP system.

If your control workstation and system is on PSSP 1.2 and AIX 3.2.5, you must first decide whether to upgrade service on all nodes. If you intend to upgrade all the

© Copyright IBM Corp. 1996

nodes directly to PSSP 2.2, then service upgrades are not needed. Service upgrades are recommended, however, for nodes that will run in AIX 3.2.5 partitions. Upgrade the node that will become the boot/install server before making it the server. You should make a mksysb system backup for system recovery.

As an option, you can create a production system partition with AIX 3.2.5 and PSSP 1.2-level software and a test system partition with AIX 4.1 and PSSP 2.2-level software. In this way, you can test AIX 4.1/PSSP 2.2 while running your existing AIX 3.2.5/PSSP 1.2 production environment. Figure 9 shows an example of how this environment could be set up. For examples of partitioning systems, see the *System Planning Guide*.

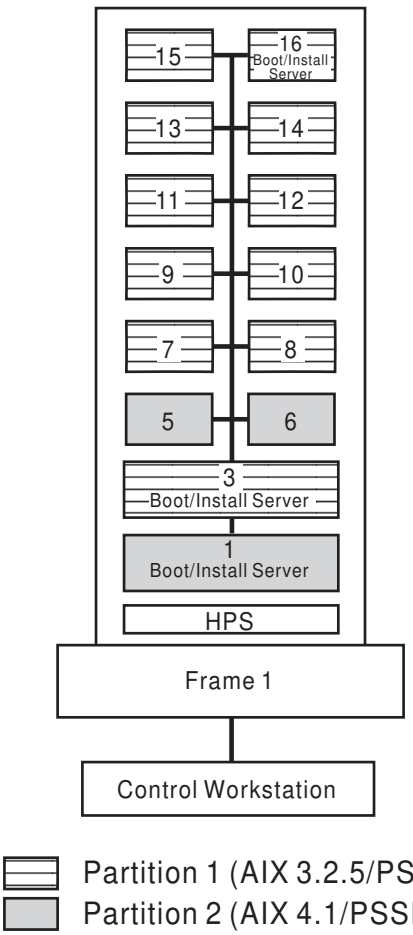

Figure 9. The Migration Environment

As you prepare for migration, keep in mind that releases earlier than the PSSP 1.2-level software are not supported in a system partition.

Step 1: Back Up Your Control Workstation

Create a **mksysb** image of your existing AIX 3.2.5/PSSP 1.2 root volume group of the control workstation.

Step 2: Back Up Important File Systems on the Control Workstation

This is an optional step but it is highly recommended.

You may also want to keep backup copies of file systems that have configuration data in them that you can mount on the migrated Control Workstation so that you can easily verify your new configuration by inspection. File systems you may want to backup include:

- /root
- /usr
- /var

Step 3: 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.

Make the boot/install server one of the nodes in an AIX 3.2.5 system partition. This saves you a step later on. The AIX 3.2.5 and PSSP 1.2 system partitions must access at least one boot/install server within any system partition so you can reinstall a node in the AIX 3.2.5 system partition in case of a hardware or software failure on the node.

Because you will not have the PSSP 1.2 software on your upgraded control workstation, a node's **mksysb** image for the AIX 3.2.5 system partitions should include all the PSSP 1.2 software you currently use in your production system partition. If your current system does not contain such a mksysb, you can create one from a production node before you migrate your system. Copy the node's **mksysb** image from an AIX 3.2.5 partition to **/usr/sys/inst.images/ssp** on the boot/install server node of the system partition, and then update the SDR to reflect the installation image name of the mksysb, if necessary. The command for updating the SDR is:

```
spbootins -i install_image_name -l node_list
```

where *install_image_name* is the name of the **mksysb** image, and *node_list* is a list of nodes this image runs on.

IBM recommends 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, you should 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*.

Note: **spbootins** must be run from the control workstation.

Caution: When the last boot/install server is upgraded, the server resources (such as mksysb images and the pssp file set) are deleted from the last remaining server. It is strongly recommended that you back up the server before doing this so that you can restore the old environment in case something goes wrong.

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 (the AIX 4.1 and PSSP 2.2 system 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 2.2 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 2.2 system partition.

Note: Nodes that are /usr clients cannot be migrated. You must change the /usr server to local for the nodes with the above spbootins command, then do a complete reinstall of AIX and PSSP in order to upgrade them.

Step 4: Verify the Control Workstation Requirements

The control workstation must have sufficient paging space and disk space for the boot/install server files. For more information, see "Step 2: Verify the Control Workstation Requirements" on page 14.

Important Notes

- Generally, completing the configuration worksheets found in the planning guide is not necessary when migrating. However, if you are going to use partitioning to implement your upgrade strategy, you may find completing the worksheets helpful because partitioning can involve moving and adding nodes.
- All tasks must be run on the control workstation as root, except where indicated.

  All of the RS/6000 SP commands in this chapter are in **/usr/lpp/ssp/bin**, except where indicated. To avoid entering the complete path name each time you want to invoke a RS/6000 SP command, add **/usr/lpp/ssp/bin** to the root user path.

Step 5: Prepare for PSSP Installation

If you chose to do an AIX migration install, complete "Step 6: Prepare for PSSP Migration Installation" on page 113 and "Step 7: Perform BOS Migration Installation on the Control Workstation" on page 113 before doing PSSP Installation and then continue with "Step 14: Verify Control Workstation Interfaces" on page 119.

If you chose an AIX overwrite or preservation install, but wish to save your PSSP configuration on the control workstation, complete "Step 8: Prepare for PSSP Reinstallation" on page 114 through "Step 13: Configure Ethernet Adapters" on page 118 and continue with "Step 14: Verify Control Workstation Interfaces" on page 119.

Be sure to install the recommended PTF levels. Check the PSSP Memo to Users for the most up to date recommendations or refer to the latest README file.

Step 6: Prepare for PSSP Migration Installation

PSSP 2.2 provides the following software migration path which preserves certain files on your PSSP 1.2 control workstation:

- An AIX 4.1 migration installation of the control workstation

Note: The **.klogin** file of the Kerberos Administrative Principal in PSSP 2.2 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
```

You do not need to run **setup_authent**. However, if the SP Authentication Services are reinitialized after installation of PSSP 2.2, you must customize all PSSP V1R2 nodes to distribute new **krb-srvtab** files to those nodes. The same migration software detects the presence of your SP Authentication Services configuration and starts the appropriate daemons.

Step 7: Perform BOS Migration Installation on the Control Workstation

Perform an AIX migration installation on the control workstation. Refer to the AIX installation guide for more information.

If you perform this step, skip “Step 8: Prepare for PSSP Reinstallation” on page 114 through “Step 13: Configure Ethernet Adapters” on page 118 and proceed with “Step 14: Verify Control Workstation Interfaces” on page 119.

Notes:

1. 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 4.1 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 an 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 RS/6000 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 8: Prepare for PSSP Reinstallation

Do this step if you are performing an overwrite or preservation install.

PSSP 2.2 provides the following software migration path which preserves certain files from your PSSP 1.2 control workstation:

- Saving a set of files from your AIX 3.2.5 control workstation and restoring them after you install AIX 4.1.

Note: The **.klogin** file of the Kerberos Administrative Principal in PSSP 2.2 contains an entry not 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.

The entry you add references a remote command (**rcmd**) principal for the control workstation. 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
```

Saving Files From Your AIX 3.2.5 Control Workstation

The following is a minimum list of the files you must save:

- The contents of /**var**/**sdr**
- The contents of /**var**/**kerberos**
- /**.k**
- /**.klogin**
- /etc/krb-srvtab
- /etc/krb.conf
- /etc/krb.realms
- /etc/hmacls
- /usr/lpp/ssp/config/hmthresholds

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 list of filenames:

   ```
   /.k
   /.klogin
   /etc/krb-srvtab
   /etc/krb.conf
   ```

/etc/krb.realms
/etc/hmacls
/usr/lpp/ssp/config/hmthresholds

2. Run the following tar command:

```
tar -cvf PSSP-1.2.tar -L MigList /var/sdr /var/kerberos
```

   This creates a tar archive of the files listed above, the SDR, and the Kerberos database.

   To verify the tar file **PSSP-1.2.tar** is readable, run the following tar command:

```
tar -tvf PSSP-1.2.tar
```

   If you prefer saving the files on tape, substitute the name of a device for **PSSP-1.2.tar** in these examples.

3. Copy **PSSP-1.2.tar** to another system or some other safe location before you install AIX 4.1 on your control workstation.

When you restore the PSSP 1.2 SDR on your AIX 4.1 control workstation, the PSSP 2.2 software detects a migration—it upgrades the saved SDR data and converts it to PSSP 2.2. You do not need to re-enter SP configuration information.

If the SP Authentication Services are reinitialized after installation of PSSP 2.2, you must customize all PSSP 2.2 nodes to distribute new **krb-srvtab** files to those nodes. The same migration software detects the presence of your SP Authentication Services configuration and starts the appropriate daemons. You do not need to run **setup_authent**.

Saving Additional Files from your AIX 3.2.5 Control Workstation

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. 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**.

Caution: Do not use the "MigList" method shown above 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, your specific changes should be carefully merged into the new versions of these files. Do not merely copy the old version of the file onto the new version.

This list is not a comprehensive list of everything that might be customized 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/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	Filesystem information
/etc/group	Basic group attributes
/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/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/passwd	Password information
/etc/services	network port services
/etc/sysctl.acl	Sysctl file for ACL priveleges
/etc/sysctl.conf	Sysctl configuration file for sysctl commands
/usr/lpp/ssp/config/hwevents	user exits for hardware state changes

Step 9: Perform BOS Install on the Control Workstation

This step is optional. Do this step if you are performing an overwrite or preservation install.

Notes:

1. 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 4.1 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 an 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 RS/6000 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 10: Restore Configuration Files

This step is optional. Do this step if you are performing an overwrite or preservation install.

Restore the PSSP files you saved in "Step 8: Prepare for PSSP Reinstallation" on page 114. Copy the archive file to the control workstation and restore the files using the command:

```
tar -xvf PSSP-1.2.tar
```

Step 11: Restore Additional Configuration Files

This step is optional. Do this step if you are performing an overwrite or preservation install.

Restore additional files saved to /tmp. Then you can reintegrate your changes into the new versions of these files.

Step 12: Configure RS-232 Control Lines

This step is optional. Do this step if you are performing an overwrite or preservation install.

Each frame in your RS/6000 SP 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.

Use SMIT or the **mkdev** command to define the RS-232 interfaces as they appear on your Control Workstation Worksheet.

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`**
Note: You can accept the default baud rate of 9600. When the SP System Monitor starts, it changes the rate to 19200.	

Step 13: Configure Ethernet Adapters

This step is optional. Do this step if you are performing an overwrite or preservation install.

Use **smit chinet** or the **chdev** command to configure each Ethernet adapter connecting your RS/6000 SP 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 accessed through the **info** command.

Refer to your RS/6000 SP Control Workstation Worksheet in the *System Planning Guide* 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.

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`

Step 14: 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 129.33.34.1 -c 1

Reconfigure the adapter if you do not receive a response.

Changing root Default Processes

When you first install your RS/6000 SP system, the number of processes the root user can have is set to **40**, an AIX 4.1 default. You will not be able to continue installing your system with this default value—you must increase the number.

To change the value, enter the following command:

chdev -l sys0 -a maxuproc='256'

Tunables and Tunable Values

Refer to “Step 11: Change Tunables and Tunable Values” on page 19 for more information.

Step 15: Define Space for NIM Boot Images

Before creating an AIX 4.1 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 16: Define Space for the /spdata Directory

Refer to “Step 13: Define Space for the /spdata Directory” on page 21 for more information.

Create Required /spdata Directories

Note: Make sure you mount the new **/spdata** file system before you create the **/spdata** directories.

The RS/6000 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`. Issue the following commands to create the required directories:

.

- mkdir /spdata/sys1

  This is the main directory for SDR, SPMON, Log Mgt, and Installation.

- mkdir /spdata/sys1/install

  This is the main directory for PSSP installation.

- mkdir /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 /spdata/sys1/install/<name>

  This is the subdirectory for the required AIX 4.1 file sets. You can choose any name but the name must not contain any dots (.). The chosen name will be updated through SMIT. By default this is set up as the string "default". You might want to pick a more meaningful name, such as aix414 for AIX 4.1.4 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.

- mkdir /spdata/sys1/install/<name>/lppsource

  This is the location of required AIX 4.1 file sets. Use the same name (or repeat with multiple names) as in the previous step.

- mkdir /spdata/sys1/install/pssplpp

  This is the location of all subdirectories for RS/6000 SP installp file sets.

- mkdir /spdata/sys1/install/pssplpp/PSSP-2.2

  This is the location of installp file sets for the code version PSSP-2.2. If the control workstation will be NIM server for nodes at other PSSP code levels, other subdirectories will be created under pssplpp with the code versions for those levels.

Step 17: Copy the AIX 4.1 LPP Images

Refer to "Step 15: Copy the AIX 4.1 LPP Images and Other Required AIX LPPs" on page 24 for complete instructions.

Step 18: Copy the PSSP Images

Refer to "Step 16: Copy the PSSP Images" on page 26 for complete instructions.

Step 19: Install the Basic AIX Image

If you have not already installed the basic AIX image, you need to do so now. Refer to "Step 17: Install a Basic AIX (mksysb) Image" on page 27.

Step 20: Install PSSP on the Control Workstation

Complete "Step 18: Install PSSP on the Control Workstation" on page 27.

Step 21: Authenticate as the Administrative Principal

Authenticate as the Kerberos administrative user. Use the command:

`kinit` *`admin_user`***`.admin`**

where *admin_user* is the name of your Kerberos administrative user.

Step 22: Complete PSSP Installation on the Control Workstation

To complete installation of the PSSP on the control workstation, enter the following command with no parameters:

```
install_cw
```

For more information, see "Step 21: Complete System Support Installation on the Control Workstation" on page 39.

Step 23: Run SDR and System Monitor Verification Test

In this step, run verification tests that check for correct installation of the SDR, correct installation of the System Monitor and correct configuration of the System Monitor.

Complete "Step 22: Run SDR and System Monitor Verification Tests" on page 40 and "Step 27: Verify System Monitor Installation" on page 45.

Step 24: Configure PSSP Services

To configure the PSSP services defined by the Site Environment information, run the following script:

/usr/lpp/ssp/install/bin/services_config.

This script initializes services if necessary and starts daemons for services including NTP and Amd.

Step 25: Set Up the Site Environment LPP Source Name

You must set the LPP Source Name to the subdirectory under **/spdata/sys1/install** where your control workstation lppsource is located. In the SMIT panel for Site Environment Information, fill this information into the field "Control Workstation LPP Source Name". By default it is set to the string "default", so if you use that as your subdirectory name you don't have to change this.

Alternatively, you could use the spsitenv command to set the lppsource name:

```
spsitenv cw_lppsource_name=<name>
```

where <*name*> is the name of the control workstation's lpp source subdirectory.

Step 26: Start System Partition-Sensitive Subsystems

There are new system partition-sensitive subsystems that need to be added to the system. Even if you are not partitioning your system, this step needs to be done since you still have one default partition.

Refer to “Step 25: Start System Partition-Sensitive Subsystems” on page 43 for complete instructions.

Step 27: Verify System Partition-Sensitive Subsystems Have Started

Refer to “Step 26: Verify System Partition-Sensitive Subsystems Have Started” on page 44 for complete instructions.

Step 28: Validate the Upgraded Control Workstation

This step is optional, but you may want to let your system run for a period of time with only the updated control workstation supporting the AIX 3.2.5 and PSSP 1.2 nodes. This indicates the stability of the upgraded control workstation at AIX 4.1 and PSSP 2.2.

Step 29: Shut Down the Nodes

Do “Step 29: Shut Down the Nodes” through “Step 33: Test PSSP 2.2” on page 124 ONLY if you are setting up system partitions.

In this step, you shut down all the nodes of your system to prepare for system partitioning. 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
Command line	Issue the **cshutdown -F ALL** command.

Step 30: Create System Partitions

Follow the procedures described in the *Administration Guide* to create the following system partitions:

- A production system partition running your existing production environment
- A test system partition to test PSSP 2.2.

Note, there is a new System Partitioning Aid that may help you create partitions, particularly if you want partition configurations other than those supplied with the PSSP.

Step 31: Reboot the Nodes in the Production System Partition

1. Reboot the nodes of your AIX 3.2.5 production partition.
2. Verify the production partition. When the nodes have booted and initialized, the production partition is ready for use.
3. If you have a switch, issue the **Estart** command in the production partition.

Step 32: Install AIX 4.1 and PSSP 2.2 in the Test System Partition

This is a full installation or a migration installation of SP software on the nodes of the test system partition. Follow the instructions starting with “Steps to Do an Overwrite Install to Upgrade to PSSP 2.2” on page 146 if you want to to a full installation. To do a migration installation, see “Migrating Nodes from PSSP 1.2 to PSSP 2.2” on page 142.

Step 33: Test PSSP 2.2

You can test the PSSP 2.2 software while also running the production system partition. The control workstation manages both system partitions. If the production system partition becomes disrupted, use the same backout procedure you would use for the control workstation applied to all the nodes in the test system partition. This procedure is described in “Step 1: Back Up Your Control Workstation” on page 110.

When you complete your testing, you can install production system nodes with the same image currently running as a test system. If problems occur in production, restore the nodes with the **mksysb** image you created.

Steps to Migrate the Control Workstation from PSSP 2.1 to PSSP 2.2

Follow the steps in this section if you have chosen the **migration** approach to upgrading from PSSP 2.1 to PSSP 2.2 as described in the migration chapter of *System Planning Guide*. If you have an HACWS Configuration, see "Strategy for HACWS Migration" on page 138 instead. Before doing these steps, quiesce all jobs and stop the Resource Manager on the RS/6000 SP system.

If your control workstation and system is on PSSP 2.1 and AIX 4.1.3, you must upgrade PSSP 2.1 nodes to AIX 4.1.4 before you migrate them to PSSP 2.2. If you plan a long migration, you may want to create AIX 4.1.3 boot servers, or AIX 4.1.3 spots, then uplevel PSSP 2.1 and AIX service on the nodes that will migrate later. Note that this procedure requires a minimal PSSP PTF. Refer to the Memo to Users for more information.

As an option, you can create a production system partition with PSSP 2.1-level software and a test system partition with PSSP 2.2-level software. In this way, you can test PSSP 2.2 while running your existing PSSP 2.1 production environment. Figure 10 shows an example of how this environment could be set up. For examples of partitioning systems, see the *System Planning Guide*.

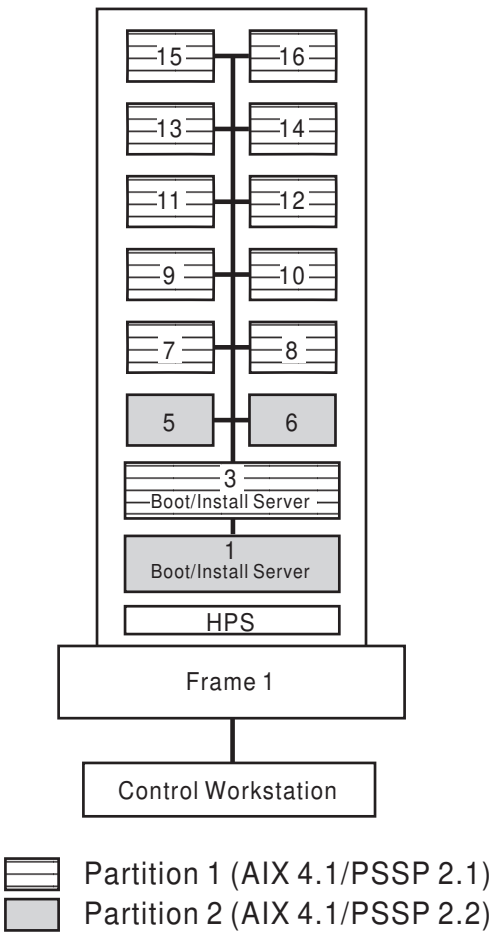

Figure 10. The Migration Environment

As you prepare for migration, keep in mind that releases earlier than the PSSP 1.2-level software are not supported in a system partition.

Step 1: Archive the SDR (optional)

Before migrating your system or making a backup it is recommended that you archive the SDR at its current level.

```
SDRArchive <some_name>

where <some_name> is the name you want to use for this archive.
```

Step 2: Back Up Your Control Workstation

Create a **mksysb** image of your existing AIX 4.1 and PSSP 2.1 root volume group of the control workstation.

Step 3: Back Up Important File Systems on the Control Workstation

This step is optional.

You may also want to keep backup copies of file systems that have configuration data in them that you can mount on the migrated Control Workstation so that you can easily verify your new configuration by inspection. File systems you may want to backup are:

- /root
- /usr
- /var
- /spdata

Step 4: Verify the Control Workstation Requirements

The control workstation must have sufficient paging space and disk space for the boot/install server files. For more information, see “Step 2: Verify the Control Workstation Requirements” on page 14.

Important Notes

- Generally, completing the configuration worksheets found in the planning guide is not necessary when migrating. However, if you are going to use partitioning to implement your upgrade strategy, you may find completing the worksheets helpful because partitioning can involve moving and adding nodes.
- All tasks must be run on the control workstation as root, except where indicated.

  All of the RS/6000 SP commands in this chapter are in **/usr/lpp/ssp/bin**, except where indicated. To avoid entering the complete path name each time you want to invoke a RS/6000 SP command, add **/usr/lpp/ssp/bin** to the root user path.

Step 5: Prepare for PSSP Installation

If you are upgrading AIX to a new version, for instance from AIX 4.1.3 to AIX 4.1.4, apply the PTF to go to AIX 4.1.4 now and skip to “Step 13: Verify Control Workstation Interfaces” on page 131. If you chose an AIX overwrite install, complete “Step 6: Prepare for PSSP Reinstallation” on page 127 through “Step 12: Configure Ethernet Adapters” on page 130.

Step 6: Prepare for PSSP Reinstallation

Before You Begin

Do this step if you are performing an AIX overwrite installation of the control workstation.

PSSP 2.2 provides the following software migration path which preserves certain files from your AIX 4.1.3 control workstation:

- Saving a set of files from your AIX 4.1.3 control workstation and restoring them after you install AIX 4.1.4

Saving Files from Your AIX 4.1.3 Control Workstation

If you are doing an AIX overwrite installation, you must save the following files if you wish to migrate PSSP.

- The contents of /**spdata**
- The contents of /**var**/**kerberos**
- /**.k**
- /**.klogin**
- /etc/krb-srvtab
- /etc/krb.conf
- /etc/krb.realms
- /etc/hmacls
- /usr/lpp/ssp/config/hmthresholds

If still have some AIX 3.2.5 nodes, you must also save the following files to preserve the **netinst** id. (Also, you might want to save these files even if you no longer have any AIX 3.2.5 nodes.)

- /etc/group
- /etc/security/group
- /etc/passwd
- /etc/security/passwd

Follow this procedure to save the PSSP files required for migration:

1. Save the contents of /spdata. If your /spdata is a separate volume group, you may export the volume group with the exportvg command. Otherwise, you should use the backup command to save the /spdata filesystem.
2. Create a file called **MigList** containing the following minimum set list of filenames:

   ```
   /.k
   /.klogin
   /etc/krb-srvtab
   /etc/krb.conf
   /etc/krb.realms
   ```

3. Run the following tar command:

   ```
   tar -cvf PSSP-2.1.tar -L MigList /var/kerberos
   ```

   This creates a tar archive of the files listed above and the Kerberos database.

   To verify the tar file **PSSP-2.1.tar** is readable, run the following tar command:

   ```
   tar -tvf PSSP-2.1.tar
   ```

If you prefer saving the files on tape, substitute the device for **PSSP-2.1.tar** in these examples.

4. Copy **PSSP-2.1.tar** to another system or some other safe location before you install AIX on your control workstation.

When you restore the PSSP 2.1 SDR on your control workstation, the PSSP 2.2 software detects a migration—it upgrades the saved SDR data and converts it to PSSP 2.2. You do not need to re-enter SP configuration information.

If the SP Authentication Services are reinitialized after installation of AIX 4.2, you must customize all PSSP 2.1 nodes to distribute new **krb-srvtab** files to those nodes. The same migration software detects the presence of your SP Authentication Services configuration and starts the appropriate daemons. You do not need to run **setup_authent**.

Saving Additional Files from your AIX 4.1 Control Workstation

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 make sure you integrate your changes into the new system. 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**.

Caution: Do not use the "MigList" method shown above 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 before using tar. After reinstalling your system, your specific changes should be carefully merged into the new versions of these files. Do not merely copy the old version of the file onto the new version.

This list is not a comprehensive list of everything that might be customized 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/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	Filesystem information
/etc/group	Basic group attributes
/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/niminfo	NIM information for installation
/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/passwd	Password information
/etc/services	network port services
/etc/splm.allow	Error Log Mgt file for splm command
/etc/sysctl.acl	Sysctl file for ACL priveleges
/etc/sysctl.conf	Sysctl configuration file for sysctl commands
/etc/tftpaccess.ctl	PSSP and NIM access for Installation

Step 7: Perform BOS Install on the Control Workstation

Do this step if you are performing an AIX overwrite installation of the control workstation. Refer to the AIX installation guide for instructions.

Step 8: Restore Configuration Files

Do this step if you did an AIX overwrite installation of the control workstation.

Restore the PSSP files you saved in “Step 6: Prepare for PSSP Reinstallation” on page 127. Copy the archive file to the control workstation and restore the files using the command:

```
tar -xvf PSSP-2.1.tar
```

Restore the configuration files you saved.

Step 9: Restore /spdata

Restore the /spdata you saved in “Step 6: Prepare for PSSP Reinstallation” on page 127. Use importvg if you saved /spdata with exportvg. Use restore if you saved /spdata with backup.

Step 10: Restore Additional Configuration Files

Do this step if you did an AIX 4.1 migration installation of the control workstation. Restore additional files saved in my.archive to /tmp.

Then you can reintegrate your changes into the new versions of these files.

Step 11: Configure RS-232 Control Lines

Do this step if you did an AIX overwrite installation of the control workstation.

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.

Use SMIT or the **mkdev** command to define the RS-232 interfaces as they appear on your Control Workstation Worksheet.

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`
Note: You can accept the default baud rate of 9600. When the SP System Monitor starts, it changes the rate to 19200.	

Step 12: Configure Ethernet Adapters

Before You Begin

Do this step if you did an AIX overwrite installation of the control workstation.

Use **smit chinet** or the **chdev** command to configure each Ethernet adapter connecting your RS/6000 SP 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 accessed through the **info** command.

Refer to your RS/6000 SP Control Workstation Worksheet in the *System Planning Guide* for the IP addresses and netmask values of your Ethernet adapters.

Note: If 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 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`

Step 13: 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 129.33.34.1 -c 1

Reconfigure the adapter if you do not receive a response.

Changing root Default Processes

When you first install your RS/6000 SP system, the number of processes the root user can have is set to **40**, an AIX 4 default. You will not be able to continue installing your system with this default value—you must increase the number.

To change the value, enter the following command:

chdev -l sys0 -a maxuproc='256'

Tunables and Tunable Values

Refer to “Step 11: Change Tunables and Tunable Values” on page 19 for more information.

Step 14: Review Space Requirements for NIM Boot Images

Before creating an AIX 4.1 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 15: Review Space Requirements for /spdata

Before You Begin

Do this step if you did an AIX overwrite installation of the control workstation.

The /**spdata** directory contains mksysb and installp file sets. IBM recommends 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 *System Planning Guide* to help you estimate how much space you need to define.

Step 16: Create Required /spdata Directories

The following subdirectories are new to PSSP 2.2. Since PSSP 2.2 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.

The RS/6000 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`. Issue the following commands to create the required directories:

- To create /spdata/sys1/install<name>, issue:

  ```
  mkdir /spdata/sys1/install/<name>
  ```

  This is the subdirectory for the required AIX 4.1.4 file sets. You can choose any name but the name must not contain any dots (.). The name you choose will be updated through SMIT. By default this is set up as the string "default". You might want to pick a more meaningful name, such as aix414 for AIX 4.1.4 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/<name>/lppsource, issue:

  ```
  mkdir /spdata/sys1/install/<name>/lppsource
  ```

  This is the location of required AIX 4.1.4 file sets. Use the same name (or repeat with multiple names) as in the previous step.

- To create /spdata/sys1/install/pssplpp/PSSP-2.2, issue:

  ```
  mkdir /spdata/sys1/install/pssplpp/PSSP-2.2
  ```

  This is the location of installp file sets for the code version PSSP-2.2. 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 (such as PSSP-2.1).

Step 17: Review the AIX 4.1.4 LPP Images

If you have not done so already, and you have a new level of AIX lppsource, you must now download the AIX file sets into the **lppsource** directory on the control workstation. You have a choice. You can download all of the AIX file sets (approximately 1.5 GB) or only the minimal required AIX file sets (approximately 450 MB)

If you already have the AIX 4.1.4 file sets, note that a new file set, perfagent.server is required.

For complete instructions, refer to "Step 15: Copy the AIX 4.1 LPP Images and Other Required AIX LPPs" on page 24.

Step 18: Move the Existing LPP Images

Since multiple SPOTs are now supported, there is a new directory structure under /**spdata**/**sys1**/**install**. If you have an existing lppsource directory under /**spdata**/**sys1**/**install**/**lppsource**, you should move the lppsource directory to a subdirectory with a name of your choice. If you choose to keep any PSSP 2.1 nodes, you also need to create a symbolic link from the location that PSSP 2.1 used to the new location. For instance, if the lppsource is for AIX 4.1.3, you could issue the following:

```
mkdir /spdata/sys1/install/aix413

mv /spdata/sys1/install/lppsource \
   /spdata/sys1/install/aix413

ln -s /spdata/sys1/install/aix413/lppsource \
      /spdata/sys1/install/lppsource
```

Step 19: Copy the PSSP Images for PSSP 2.2

Refer to "Step 16: Copy the PSSP Images" on page 26 for complete instructions.

Step 20: Move the PSSP Images for PSSP 2.1

If any of your nodes will remain at the PSSP 2.1 level, you also need those PSSP images. If they do not exist on your system now (for instance if you did an overwrite installation of AIX and did not preserve them), use the above method to load them from your installation media. Put them in the /**spdata**/**sys1**/**install**/**pssplpp**/**PSSP-2.1** directory.

If the /**spdata**/**sys1**/**install**/**pssplpp** directory still exists from your PSSP 2.1 control workstation, issue the following commands:

- mkdir /spdata/sys1/install/pssplpp/PSSP-2.1
- mv /spdata/sys1/install/pssplpp/pssp.installp /spdata/sys1/install/pssplpp/PSSP-2.1

Also move any other LPPs that you have in the /spdata/sys1/install/pssplpp directory.

If you choose to keep any PSSP 2.1 nodes, you will also need to create a symbolic link from the location that PSSP 2.1 used to the new location. Issue:

```
ln -s /spdata/sys1/install/pssplpp/PSSP-2.1/pssp.installp \
      /spdata/sys1/install/pssplpp/pssp.installp
```

Step 21: Install the Basic AIX Image

If you have not already installed the basic AIX image, you need to do so now. First move the existing image to another name to save it. For instance, issue:

```
mv /spdata/sys1/install/images/bos.obj.ssp.41 \
   /spdata/sys1/install/images/bos.obj.ssp.41.old
```

Then refer to "Step 17: Install a Basic AIX (mksysb) Image" on page 27.

Step 22: Stop Daemons on the Control Workstation

Refer to the following table for the commands to issue to stop the daemons from running on the control workstation:

To stop this daemon:	Issue this command:
sdrd daemons	`stopsrc -g sdr`
sysctld daemon	`stopsrc -s sysctld`
hardmon daemon	`stopsrc -s hardmon`
splogd daemon	`stopsrc -s splogd`
hr daemons	`stopsrc -g hr`
hb daemons	`stopsrc -g hb`
Emonitor daemon	`stopsrc -g emon`

Step 23: Verify that the Daemons are Not Running

Issue **lssrc -a** to verify that the daemons are not active.

Step 24: Install PSSP on the Control Workstation

Complete "Step 18: Install PSSP on the Control Workstation" on page 27.

Step 25: Authenticate as the Administrative Principal

Authenticate as the Kerberos administrative user. Use the command:

```
kinit admin_user.admin
```

where *admin_user* is the name of your Kerberos administrative user.

Step 26: Complete PSSP Installation on the Control Workstation

To complete installation of the PSSP on the control workstation, enter the following command with no parameters:

```
install_cw
```

For more information, see "Step 21: Complete System Support Installation on the Control Workstation" on page 39.

Step 27: Run SDR and System Monitor Verification Test

In this step, run verification tests that check for correct installation of the SDR, correct installation of the System Monitor and correct configuration of the System Monitor.

Complete “Step 22: Run SDR and System Monitor Verification Tests” on page 40 and “Step 27: Verify System Monitor Installation” on page 45.

Step 28: Configure PSSP Services

To configure the PSSP services defined by the Site Environment information, run the following script:

/usr/lpp/ssp/install/bin/services_config

This script initializes services if necessary and starts daemons for services including NTP and Amd.

Step 29: Set Up the Site Environment LPP Source Name

You must set the LPP Source Name to the subdirectory under /spdata/sys1/install where your control workstation lppsource is located. In the SMIT panel for Site Environment Information, fill this information into the field "Control Workstation LPP Source Name". By default is is set to the string "default", so if you use that as your subdirectory name you don't have to change this.

Alternatively, you could use the spsitenv command to set the lppsource name:

```
spsitenv cw_lppsource_name=<name>
```

where <*name*> is the name of the control workstation's lpp source subdirectory.

Step 30: Start System Partition-Sensitive Subsystems

There are new system partition-sensitive subsystems that need to be added to the system. Even if you are not partitioning your system, this step needs to be done since you still have one default partition. Do the following:

1. Remove the old subsystems (hr, hb and emonitor) by issuing **syspar_ctrl -c** <**subsystem name**>.
2. Add the new subsystems. Refer to “Step 25: Start System Partition-Sensitive Subsystems” on page 43 for complete instructions.

Step 31: Verify System Partition-Sensitive Subsystems Have Started

Refer to “Step 26: Verify System Partition-Sensitive Subsystems Have Started” on page 44 for complete instructions.

Step 32: Unconfigure the NIM Master

If you did an overwrite install, skip this step. Otherwise, since PSSP 2.2 supports multiple SPOTs rather than one /usr SPOT as in PSSP 2.1, you need to unconfigure the NIM master by issuing the following command:

```
delnimmast -l 0
```

Step 33: Configure Control Workstation as Boot/Install Server

Perform this step only if you are not going to partition your system at this time. Otherwise, **setup_server** will be run after your partitions are defined.

Run **setup_server** by specifying "yes" on the SMIT Boot/install/usr Server Information panel, or by running it on the command line.

Step 34: Validate the Upgraded Control Workstation

This step is optional, but you may want to let your system run for a period of time with only the updated control workstation supporting the AIX 4.1 and PSSP 2.1 nodes. This indicates the stability of the upgraded control workstation at AIX 4.1.4 and PSSP 2.2.

Step 35: Shut Down the Nodes

Before You Begin

Do "Step 29: Shut Down the Nodes" on page 122 through "Step 33: Test PSSP 2.2" on page 124 ONLY if you are setting up system partitions. Note, there is a new System Partitioning Aid that may help you create partitions, particularly if you want partition configurations other than those supplied with the PSSP.

In this step, you shut down all the nodes of your system to prepare for system partitioning.

If using:	Do this:
System Monitor GUI	**SELECT** the System Monitor Global Control Display **SELECT** the All and Shutdown options
Perspectives	**SELECT** the Hardware icon by double clicking on it. **SELECT** the nodes to be powered off. **PRESS** Power Off icon from the Tool Bar **SELECT** cshutdown **PRESS** Apply
Command line	Issue the **cshutdown -F All** command.

Step 36: Create System Partitions

Follow the procedures described in the *Administration Guide* to create the following system partitions:

- A production system partition running your existing production environment
- A test system partition to test PSSP 2.2.

Step 37: Reboot the Nodes in the Production System Partition

1. Reboot the nodes of your PSSP 2.1 production partition.
2. Verify the production partition. When the nodes have booted and initialized, the production partition is ready for use.
3. If you have a switch, issue the **Estart** command in the production partition.

Step 38: Install AIX 4.1 and PSSP 2.2 in the Test System Partition

This is a full installation or a migration installation of SP software on the nodes of the test system partition. Follow the instructions starting with "Step 44: Network Boot Optional Boot/Install Servers" on page 70 if you want to to a full installation. To do a migration installation, see "Migrating Nodes from PSSP 2.1 to PSSP 2.2" on page 144.

Step 39: Test PSSP 2.2

You can test the PSSP 2.2 software while also running the production system partition. The control workstation manages both system partitions. If the production system partition becomes disrupted, use the same backout procedure you would use for the control workstation applied to all the nodes in the test system partition. This procedure is described in “Step 1: Back Up Your Control Workstation” on page 110.

When you complete your testing, you can install production system nodes with the same image currently running as a test system. If problems occur in production, restore the nodes with the **mksysb** image you created.

Strategy for HACWS Migration

This chapter describes two different strategies for migrating your SP system to PSSP 2.2. The first involves saving selected configuration files, performing an overwrite or preservation install of the AIX base operating system, and restoring the saved configuration files. The second strategy involves performing a migration install of the AIX base operating system. HACWS at the PSSP 2.2 level requires HACMP 4.2, and since migration install is the recommended method for upgrading to HACMP 4.2, migration install is also the recommended method for upgrading an HACWS configuration to PSSP 2.2.

An HACWS configuration at the PSSP 2.2 level requires the following minimum software levels on both control workstations:

- AIX 4.1.4
- HACMP 4.2
- PSSP 2.2

It is not necessary to upgrade all three of these at the same time. In fact, you are encouraged to upgrade each separately. You can run AIX 4.1.4 with HACMP 4.1 and PSSP 2.1, so if you are currently running AIX 4.1.3, you may want to upgrade to AIX 4.1.4 first, and then make sure your configuration is stable before upgrading further. Once both control workstations are stable at AIX 4.1.4, you can upgrade to HACMP 4.2 while still running PSSP 2.1, and then make sure your HACWS configuration is stable before upgrading to PSSP 2.2. Once AIX 4.2 is supported by both HACMP 4.2 and PSSP 2.2, you may still wish to make sure your HACWS configuration is stable with PSSP 2.2 and HACMP 4.2 running on top of AIX 4.1.4 before upgrading to AIX 4.2. Upgrading each of these three major components separately will help to maintain the stability of your HACWS configuration.

Migrating an HACWS Configuration from PSSP 2.1 to PSSP 2.2

Step 1: Back Up Your HACWS Configuration

Create mksysb images of both control workstations, and back up the external volume group which contains the shared **/spdata** filesystem.

Step 2: Back Up Important File Systems on the Control Workstations

This step is optional.

You may also want to keep backup copies of file systems that have configuration data in them that you can mount on the migrated control workstations, so that you can easily verify your new configuration by inspection. File systems you may want to backup are:

- / (root)
- /usr
- /var
- /spdata

Step 3: Install AIX 4.1.4 on Both Control Workstations

If the control workstations are not already running AIX 4.1.4, then you need to upgrade to AIX 4.1.4 on both control workstations. Refer to the AIX Installation Guide for instructions. You may want to run at the new AIX level for a short period of time to make sure your HACWS configuration is stable before continuing to the next step.

After you upgrade to AIX 4.1.4, you can verify your HACWS configuration by running the **/usr/sbin/hacws/hacws_verify** command. This command requires the primary control workstation to be the active control workstation, or the one that is providing control workstation services. (You can find SMIT panel and command line information for **hacws_verify** in the HACWS Installation chapter.)

Step 4: Install HACMP 4.2 on Both Control Workstations

If the control workstations are not already running HACMP 4.2, then you need to upgrade to HACMP 4.2 on both control workstations. Refer to the HACMP Installation Guide for instructions. You may want to run at the new HACMP level for a short period of time to make sure your HACWS configuration is stable before continuing to the next step.

After you upgrade to HACMP 4.2, you can verify your HACWS configuration by running the **/usr/sbin/hacws/hacws_verify** command. This command requires the primary control workstation to be the active control workstation, or the one that is providing control workstation services. (You can find SMIT panel and command line information for **hacws_verify** in the HACWS Installation chapter.)

Step 5: Create Required /spdata Directories

Follow the instructions in “Step 16: Create Required /spdata Directories” on page 132.

Step 6: Copy the AIX 4.1.4 LPP Images to the Control Workstation

Follow the instructions in “Step 17: Review the AIX 4.1.4 LPP Images” on page 132.

Step 7: Move the Existing LPP Images

Follow the instructions in “Step 18: Move the Existing LPP Images” on page 133.

Step 8: Copy the PSSP 2.2 Images

Follow the instructions in “Step 19: Copy the PSSP Images for PSSP 2.2” on page 133.

Step 9: Move the PSSP 2.1 Images

Follow the instructions in “Step 20: Move the PSSP Images for PSSP 2.1” on page 133.

Step 10: Install the Basic AIX Image

Follow the instructions in “Step 21: Install the Basic AIX Image” on page 134.

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 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
```

After issuing the command, 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 2.2 on Both Control Workstations

You need to install PSSP 2.2 on both control workstations. When you invoke the installp command to install PSSP 2.2, either directly or through SMIT, some files will be copied to the /**spdata**/**sys1** directory. At this point the shared /**spdata** filesystem is mounted on the primary control workstation. Files copied to the /**spdata**/**sys1** directory on the primary control workstation get written to the shared /**spdata** filesystem. Since the shared /**spdata** file system is not available on the

backup control workstation, files copied to the /**spdata**/**sys1** directory on the backup control workstation probably get written to the / (or root) filesystem.

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 by the **install_hacws** command in step 15. In the meantime, you need to make sure there is at least 4 MB of free space in the filesystem which contains the /**spdata**/**sys1** directory, before you install PSSP 2.2 on the backup control workstation. Otherwise, the installp command may fail.

Step 14: Authenticate as the Administrative Principal

Follow the instructions in “Step 25: Authenticate as the Administrative Principal” on page 134.

Step 15: Complete PSSP 2.2 Installation on Both Control Workstations

Run the **install_hacws** command. Refer to the HACWS chapter for SMIT and command line examples.

Step 16: Verify the HACWS Configuration

Run the **hacws_verify** command. Refer to the HACWS installation chapter for SMIT and command line examples.

Step 17: Run SDR and System Monitor Verification Tests

Follow the instructions in “Step 27: Run SDR and System Monitor Verification Test” on page 134.

Step 18: Set Up the Site Environment LPP Source Name

Follow the instructions in “Step 29: Set Up the Site Environment LPP Source Name” on page 135.

Step 19: Unconfigure the NIM Master

Follow the instructions in “Step 32: Unconfigure the NIM Master” on page 135.

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 following command on the backup control workstation:

```
    /usr/sbin/hacws/spcw_apps -u
```

Complete the rest of "Steps to Migrate the Control Workstation from PSSP 2.1 to PSSP 2.2", starting with “Step 34: Validate the Upgraded Control Workstation” on page 136.

Migrating Nodes from PSSP 1.2 to PSSP 2.2

If your control workstation and system is on PSSP 1.2 and AIX 3.2.5, you must first decide whether to upgrade service on all nodes. If you intend to upgrade all the nodes directly to PSSP 2.2, then service upgrades are not needed. Service upgrades are recommended, however, for nodes that will run in AIX 3.2.5 partitions. Upgrade the node that will become the boot/install server before making it the server. You should make a mksysb system backup for system recovery.

You need to decide if you would like to do a complete overwrite install of AIX (and PSSP) on the nodes that are being updated to PSSP 2.2, or choose the migration approach. If you choose the migration approach do "Steps to Migrate Nodes from PSSP 1.2 to PSSP 2.2" To do a complete overwrite install of a node do "Steps to Do an Overwrite Install to Upgrade to PSSP 2.2" on page 146

Steps to Migrate Nodes from PSSP 1.2 to PSSP 2.2

When migrating to PSSP 2.2, there is a new AIX migration install option that you can choose. If you use this install option, the PSSP 2.2 upgrade will also be a migration install. This means that it will replace the earlier PSSP level. You can change the **script.cust** file to install additional PSSP options that you want in your system.

Step 1: Set Up the lpp_source and PSSP Code Version

Set up the name of the lpp_source for the node. Use the subdirectory name that you loaded the lpp_source into under /spdata/sys1/install. Using SMIT:

TYPE SMIT

SELECT RS/6000 Sp System Management

SELECT RS/6000 SP Configuration Database Management

SELECT Enter Database Information

SELECT Node Database Information

SELECT Boot/Install/usr Server Information

Fill in the node numbers and LPP Source Name in the appropriate places. Choose F4 (List) for PSSP Level and select PSSP-2.2. Do not run setup_server yet; (Select "No" for that item.) Press Enter to make the changes.

You could also set up the lpp_source and PSSP code versions for the nodes with the following command:

```
spbootins -p PSSP-2.2 -l <node_list> -s no -v <name>
```

where <*name*> is the new lpp_source name for the nodes (such as aix414 if that is what you called the subdirectory with the AIX 4.1.4 lpp source).

Step 2: Set the Node(s) to Migrate

Set the boot/install server's bootp response to "migrate" with the following command:

```
spbootins -r migrate -l <node_list> -s no
```

Step 3: Verify Boot Setup

Make sure the nodes are set to migrate and that they have the correct lppsource_name and code version by issuing the following commands:

```
splstdata -G -b
splst_versions -G -t
```

Step 4: Run setup_server to configure the changes.

If this is the first time setup_server is run after installing the control workstation, it may take a long time since it will be creating the NIM master.

Step 5: Network Boot the Node or Nodes

Network Boot the node or nodes being migrated through the Perspectives GUI or by using the **nodecond** command.

Step 6: Wait for Network Boot to Finish

You can tell when the Network Boot has finished when the nodes' LEDs are blank.

Step 7: Refresh System Partition-Sensitive Subsystems

Since new levels of partition-sensitive subsystems (hb and hats) will be running on the nodes, the partition-sensitive subsystems on the control workstation should be refreshed to recognize them. On the control workstation, issue:

```
syspar_ctrl -r -G
```

Migrating Nodes from PSSP 2.1 to PSSP 2.2

If your control workstation and system is on PSSP 2.1 and AIX 4.1.3, you must upgrade PSSP 2.1 nodes to AIX 4.1.4 before you migrate them to PSSP 2.2. If you plan a long migration, you may want to create AIX 4.1.3 boot servers, or AIX 4.1.3 spots, then uplevel PSSP 2.1 and AIX service on the nodes that will migrate later. Note that this procedure requires a minimal PSSP PTF. Refer to the Memo to Users or to the latest README file.

To upgrade your nodes to PSSP 2.2 you may migrate PSSP, or choose to do a complete overwrite of AIX and PSSP. If you choose the migration approach, do "Steps to Migrate Nodes from PSSP 2.1 to PSSP 2.2" To do an overwrite install, do "Steps to Do an Overwrite Install to Upgrade to PSSP 2.2" on page 146.

Steps to Migrate Nodes from PSSP 2.1 to PSSP 2.2

Step 1: Upgrade the Node or Nodes to AIX 4.1.4

If the nodes being migrated to PSSP 2.2 are not already at AIX 4.1.4, upgrade them now.

Step 2: Set Up the lpp_source and PSSP Code Version

Set up the name of the lpp_source for the node. Use the subdirectory name that you loaded the lpp_source into under /spdata/sys1/install. Note: If the node or nodes you are migrating are already using AIX 4.1.4 you might only need to change the PSSP code version. Using SMIT:

TYPE SMIT

SELECT RS/6000 Sp System Management

SELECT RS/6000 SP Configuration Database Management

SELECT Enter Database Information

SELECT Node Database Information

SELECT Boot/Install/usr Server Information

Fill in the node numbers and LPP Source Name in the appropriate places. Choose F4 (List) for PSSP Level and select PSSP-2.2. Do not run setup_server yet; (Select "No" for that item.) Press Enter to make the changes.

You could also set up the lpp_source and PSSP code versions for the nodes with the following command:

```
spbootins -p PSSP-2.2 -l <node_list> -s no -v <name>
```

where <*name*> is the new lpp_source name for the nodes (such as aix414 if that is what you called the subdirectory with the AIX 4.1.4 lpp source).

Step 3: Set the Node or Nodes to Customize

Set the node or nodes to "customize" with the following command:

```
spbootins -r customize -l <node_list> -s no
```

Step 4: Verify Boot Setup

Make sure the nodes are set to customize and that they have the correct lppsource_name and code version by issuing:

```
splstdata -b
splst_versions -G -t
```

Step 5: Run setup_server to Configure the Changes

Issue the **setup_server** command.

Step 6: Copy the PSSP 2.2 pssp_script to Nodes' /tmp

Copy the PSSP 2.2 version of pssp_script to the /**tmp** directory on each of the nodes to be updated. If you are only updating one node, you can issue **rcp** to copy pssp_script. If you are updating multiple nodes, use a **dsh** command. For example:

```
dsh -N <ng> /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 <*ng*> is the name of a node group.

Note: These examples use node groups to act upon multiple nodes. You could also use dsh collections. Node groups must be created before being used (see the ngcreate command in the PSSP Command and Technical Reference).

Step 7: Execute the pssp_script on the Node(s)

Execute the pssp_script that you copied to /**tmp** on the node(s) you are migrating:

```
dsh -N <ng> /tmp/pssp_script
```

Step 8: Wait for pssp_script to Finish

To determine if pssp_script is running on the nodes, monitor the 3 digit LEDs.

Step 9: Start System Partition-Sensitive Subsystems

Do the following:

1. Remove the old subsystems (hr, hb) by issuing:

   ```
   dsh -N <ng> /usr/lpp/ssp/bin/syspar_ctrl -c <subsystem name>
   ```

   for the hr and hb subsystems.

2. Add and start system partition-sensitive subsystems by issuing the following command:

   ```
   dsh -N <ng> /usr/lpp/ssp/bin/syspar_ctrl -A
   ```

Step 10: Refresh System Partition-Sensitive Subsystems

Since new levels of partition-sensitive subsystems (hb and hats) will be running on the nodes, the partition-sensitive subsystems on the control workstation should be refreshed to recognize them. On the control workstation, issue:

```
syspar_ctrl -r -G
```

Steps to Do an Overwrite Install to Upgrade to PSSP 2.2

A migration path is supported to upgrade nodes to PSSP 2.2. However, if you choose to do a complete install of your nodes, you can accomplish this with the following procedure.

Step 1: Set Up the lpp_source and PSSP Code Version

Set up the name of the lpp_source for the node. Use the subdirectory name that you loaded the lpp_source into under /spdata/sys1/install. Using SMIT:

TYPE SMIT

SELECT RS/6000 Sp System Management

SELECT RS/6000 SP Configuration Database Management

SELECT Enter Database Information

SELECT Node Database Information

SELECT Boot/Install/usr Server Information

Fill in the node numbers and LPP Source Name in the appropriate places. Choose F4 (List) for PSSP Level and select PSSP-2.2. Do not run setup_server yet; (Select "No" for that item.) Press Enter to make the changes.

You could also set up the lpp_source and PSSP code versions for the nodes with the following command:

```
spbootins -p PSSP-2.2 -l <node_list> -s no -v <name>
```

where <*name*> is the new lpp_source name for the nodes (such as aix414 if that is what you called the subdirectory with the AIX 4.1.4 lpp source).

Step 2: Set the Node(s) to Install

Set the boot/install server's bootp response to "install" with the following command:

```
spbootins -r install -l <node_list> -s no
```

Step 3: Verify Boot Setup

Make sure the nodes are set to migrate and that they have the correct lppsource_name and code version by issuing:

```
splstdata -G -b
splst_versions -G -t
```

Step 4: Run setup_server to configure the changes.

If this is the first time setup_server is run after installing the control workstation, it may take a long time since it will be creating the NIM master.

Step 5: Network Boot the Node or Nodes

Network Boot the node or nodes being migrated through the Perspectives GUI or by using the **nodecond** command.

Step 6: Wait for Network Boot to Finish

You can tell when the Network Boot has finished when the nodes' LEDs are blank.

Step 7: Refresh Partition-Sensitive Subsystems

Since new levels of partition-sensitive subsystems (hb and hats) will be running on the nodes, the partition-sensitive subsystems on the control workstation should be refreshed to recognize them. On the control workstation, issue:

```
/usr/lpp/ssp/bin/syspar_ctrl -r -G
```

Coexistence with PSSP 2.2 and Earlier Releases

PSSP 2.2 supports coexistence in the same system partition with PSSP 1.2 nodes or with PSSP 2.1 nodes. This special migration support is documented in a technical bulletin available on the RS/6000 home page on the World Wide Web and through your IBM marketing representative. The bulletin is titled *Implementing Coexistence with PSSP 2.2* and is available in:

```
http://www.rs6000.ibm.com/tech/
```

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.

This chapter includes the following tasks:

Adding a Frame 150
Deleting a Frame 152
Adding Nodes 155
Deleting Nodes 157
Replacing a Node with an Equivalent Node 159
Replacing a Node with a Different Type of Node 162
Adding a Switch 165
Reconfiguring Your System for Use with the SP Switch 169
Replacing the Frame Supervisor 178
Replacing a Fixed Disk 179
Replacing a Disk Not in rootvg 180
Replacing an I/O Planar Card in a Thin Node or an Ethernet Adapter in a Wide or 604 High Node 181

Important Note!

It is very important that you consult the planning guide prior to reconfiguring your system to understand the implications of adding, deleting, or modifying any hardware.

© Copyright IBM Corp. 1996

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 *System Planning Guide*. Both the *Site Planning Guide* and the *System Planning Guide* offer information to help you with these decisions.

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 recommends 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 15 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 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 24: 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 28: Verify Frame Information” on page 45.

Step 7: Update the State of the Supervisor Microcode

Refer to “Step 29: Update the State of the Supervisor Microcode” on page 46 for more information.

Step 8: Add Nodes to the System

1. To complete this task, follow installation steps “Step 29: Update the State of the Supervisor Microcode” on page 46 through “Step 24: Enter Frame Information and Reinitialize the SDR” on page 42 and “Step 27: Verify System Monitor Installation” on page 45 and proceeding through the rest of the chapter.

   Note: Because you are adding a new frame, you must do “Step 37: 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 transfer it to one of 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 32-node topology file. If you remove a frame containing 16 nodes, you need to select a 16-node topology file. From within the topology file, you also need to select a new partition. For more information, refer to the Administration Guide and Planning Guide.

IBM recommends 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
Command line	Issue the **jm_stop** command. Refer to the Command Reference Guide for syntax information.

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 Partition

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
Command line	Issue the **cshutdown** command.

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.
Command line	This example deletes the last two frames in a four-frame system: `spdelfram -G 3 2`

See the **spdelfram** man page for more information.

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 Perspectives

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
Command line	Issue the **jm_start** command. Refer to the Command Reference Guide for syntax information.

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 *System Planning Guide*.

Before You Begin

- 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.
- 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 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 29: Update the State of the Supervisor Microcode” on page 46 for more information.

Step 3: Set Up, Power, and Configure the Nodes

1. To complete this task, follow the installation steps starting at “Step 30: Enter Required Node Information” on page 47 and proceed through the rest of the chapter.

   Notes:

   a. Only the new node needs to be selected in “Step 30: Enter Required Node Information” on page 47. Any production nodes chosen will be powered off.

   b. Only the new node needs to be selected in “Step 31: Acquire Hardware Ethernet Addresses” on page 49. Any production nodes chosen will be powered off and rebooted.

   c. If you have a switch and are using system partitions, in “Step 33: Configure Additional Adapters for Nodes” on page 51 the starting node is the first node in the system partition and the total number of nodes is the number of nodes in the system partition.

   d. When you add a node, you must run setup_server on the control workstation (see “Step 37: 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 and 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

Before You Begin

- 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.

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.
Command line	Issue the **jm_stop** command. Refer to the Command Reference Guide for syntax information.

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
Command line	Issue the **cshutdown** command.

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**
Command Line	To delete the SDR information for the 16 nodes in frame 3, enter: `spdelnode 3 1 16`

See the *Commands and Technical Reference* for more information on **spdelnode**.

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
Command line	Issue the **jm_start** command. Refer to the Command Reference Guide for syntax information.

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 an 604 high node node with another 604 high node node, you must also ensure that the microcode level of the 604 high node node is correct. Refer to “Step 29: Update the State of the Supervisor Microcode” on page 46 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, you may need to transfer the boot/install server to one of the remaining frames.

Before You Begin

- 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
Command line	Issue the **cshutdown** command.

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 29: Update the State of the Supervisor Microcode” on page 46.

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.

Important Note

If you have information for the node being replaced in **/etc/bootptab.info**, be sure to remove it, and then add the new Ethernet address.

Use SMIT or the **sphrdwrad** command to write the hardware Ethernet address to the SDR.

See "Step 31: Acquire Hardware Ethernet Addresses" on page 49 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

To restart Perspectives, issue **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 82 for a listing of information on the procedures for setting up these 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.

Before You Begin

- 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, 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 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.

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
Command line	Issue the **cshutdown** command.

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
Command line	Issue the **jm_stop** command. Refer to the Command Reference Guide for syntax information.

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**
Command Line	To delete the SDR information for the 16 nodes in frame 3, enter: `spdelnode 3 1 16`

See *Commands and Technical Reference* for more information on **spdelnode**.

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 29: Update the State of the Supervisor Microcode” on page 46 for more information.

If you are replacing a node with an 604 high node node, you need to ensure that the microcode level on the 604 high node node is correct. For more information, refer to “Step 29: Update the State of the Supervisor Microcode” on page 46.

Step 8: Set Up, Power, and Configure the Nodes

To complete this task, follow the installation steps starting at “Step 30: Enter Required Node Information” on page 47 and proceed through the rest of the chapter.

Note: When you add a node, you must complete “Step 37: 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
Command line	Issue the **jm_start** command. Refer to the Command Reference Guide for syntax information.

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 which frames the switch supports and record your information on the Switch Configuration Worksheet, located in the *System Planning Guide*. Both the *Site Planning Guide.* and the *System Planning Guide* 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.

Before You Begin

- 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 to which you add the switch.

Adding a Switch to a Switchless System

Step 1: Redefine the System to a Single Partition

Refer to the *System Planning Guide* 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: 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 33: Configure Additional Adapters for Nodes” on page 51 for more information.

Step 5: Update the State of the Supervisor Microcode

Refer to “Step 29: Update the State of the Supervisor Microcode” on page 46 for more information.

Step 6: Reconfigure the Hardware Monitor to Recognize the New Switch

To do this, issue the following command:

```
hmcmds -G setid 1:0
```

Step 7: Update the System Data Repository

To update the SDR switch information, issue **hmreinit**.

Step 8: Set Up the Switch

Do installation steps “Step 40: Set Up the Switch” on page 64 through “Step 43: Set Up System Partitions” on page 69. If you have set up system partitions, you need to reconfigure them.

Step 9: 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 10: 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 11: Reboot All Nodes

1. Reboot the nodes of your AIX 3.2.5 production partition.
2. Verify the production partition. When the nodes have booted and initialized, the production partition is ready for use.
3. If you have a switch, issue the **Estart** command in the production partition.

Step 12: Start Up and Verify the Switch

1. To complete this step, follow the installation steps starting at “Step 49: Start the Optional Switch” on page 78 and proceed through the rest of the chapter.
2. Exit the SP System Monitor GUI. To restart the SP System Monitor GUI, enter:

   spmon -g To restart Perspectives, enter:

   perspectives

Adding a Switch to a System With Existing Switches

Step 1: Redefine the System to a Single Partition
Refer to the *System Planning Guide* 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 29: Update the State of the Supervisor Microcode” on page 46 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 33: Configure Additional Adapters for Nodes” on page 51 for more information.

Step 5: Set Up the Switch
Do installation steps “Step 40: Set Up the Switch” on page 64 through “Step 43: 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" with the following command:

spbootins -r customize -l <*node_list*>

Step 8: Reboot All Nodes
1. Reboot the nodes of your AIX 3.2.5 production partition.
2. Verify the production partition. When the nodes have booted and initialized, the production partition is ready for use.
3. If you have a switch, issue the **Estart** command in the production partition.

Step 9: Start Up and Verify the Switch

1. To complete this step, follow the installation steps starting at “Step 49: Start the Optional Switch” on page 78 and proceed through the rest of the chapter.
2. Exit the SP System Monitor GUI. To restart the SP System Monitor GUI, enter:

   spmon -g To restart Perspectives, enter:

   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 165.

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 4.1.4 and PSSP 2.2. For instructions, refer to Chapter 4, “Migrating to the Latest Level of PSSP” on page 109.
- Ensure that you have the PDU or SEPBU twin tailed frame supervisor card with an installed supervisor level card of 0606 level or greater.

Step 1: Prepare for the Switch Transfer

IBM recommends 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
Command line	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	**Using SMIT**
TYPE smit syspar	**TYPE** smit syspar
SELECT Restore System Partition Configuration	**SELECT** Select System Partition Configuration
ENTER The name of a previously archived system partition configuration or press **List** for a list of choices.	Δ A list of system partition configurations appears.
PRESS Enter to apply the new configuration.	**SELECT** a single system partition
Using the command line	**Using the command line**
The full pathname of the **sprestore_config** command is:	Issue the **spapply_config** command. For more information on this command, refer to either the IBM RISC System/6000 Scalable POWERparallel Systems: SP Administration Guide or the IBM RISC System/6000 Scalable POWERparallel Systems: Command and Technical Reference.
`/usr/lpp/ssp/bin/sprestore_config <archived file>`	

Note: IBM recommends 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: **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
Command line	Issue the **cshutdown** command.

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*>**&colon.0**

   For example:

   ```
   hmcmds -G setid 1:0
   ```

Step 5: Update the State of the Supervisor Microcode

Refer to “Step 29: Update the State of the Supervisor Microcode” on page 46 for more information.

Step 6: Update the System Data Repository

To update the SDR switch information, issue **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**
Command Line	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`

See the *Commands and Technical Reference* for more information on **Eannotator**.

Storing the Switch Topology File in the SDR

Before You Begin

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 Δ 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**
Command Line	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`**

See the *Commands and Technical Reference* for more information on **Etopology**.

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**
Command Line	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.

See the *Commands and Technical Reference* for command syntax.

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 *System Planning Guide* for the Eclock topology file names.

If using:	Do this:
Perspectives	**SELECT** the Cluster_Mgmt icon Δ 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**
Command Line	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. See the *Commands and Technical Reference* for more information on the **Eclock** command.
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

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" 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:

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 Δ The Nodes Pane receives focus. **SELECT** View → Monitor Δ The Set Monitoring for Nodes dialog box appears. **SELECT** the switch_responds condition **PRESS** Apply Δ 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.
Command Line	Issue the **Estart** command.

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.
Command Line	Enter the **CSS_test** command.

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*>**&colon.0** For example:

```
hmcmds setid 1:0
```

Step 3: Update the State of the Supervisor Microcode

Refer to “Step 29: Update the State of the Supervisor Microcode” on page 46 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.

Replacing a Fixed Disk

This procedure applies only to disks that are part of the **rootvg** volume group.

Before You Begin

- 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 *Commands and Technical Reference* for more information on **kinit**.
- 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:
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** the node to power off **PRESS** Power Off icon **SELECT** the power off options **PRESS** Apply

Step 2: Replace the Disk

Your IBM Customer Engineer performs this step.

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`.

See the *Commands and Technical Reference* for **spbootins** command syntax.

Step 4: Network Boot the Node

Use the SP System Monitor GUI or Perspectives to network boot the node.

If using:	Do this:
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.
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.	

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:
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** the node to power off **PRESS** Power Off icon **SELECT** the power off options **PRESS** Apply

Step 2: Replace the Failing Fixed Disk

Your IBM Customer Engineer performs this step for you.

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

Replacing an I/O Planar Card in a Thin Node or an Ethernet Adapter in a Wide or 604 High Node

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.

Before You Begin

- A ticket is required to perform some of the commands in this procedure. Run the **kinit** command. See the *Commands and Technical Reference* for more information on **kinit**.
- 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:
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** the node to power off
	PRESS Power Off icon
	SELECT the power off options
	PRESS Apply

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. For example, to delete the boot/install server for node number 3, issue:

```
delnimclient -l 3
```

Step 4: Obtain the New Hardware Ethernet Address

Important Note

If you have information for the node being replaced in /**etc**/**bootptab.info**, be sure to remove it.

Use the **sphrdwrad** command to get the new hardware Ethernet address. See the *Commands and Technical Reference* for command syntax.

Chapter 6. Performing Software Maintenance

This chapter provides information on updating installation images, LPPs, and support programs. It includes the following topics:

Installing Program Updates 183
Reinstalling PSSP 185
Updating the Print Subsystem 185
Installing Updates on a Per Node Basis 185
Installing Updates through Reinstallation 186
Applying PTFs to the SP System 188
Restoring a Control Workstation from mksysb Image 190

Installing Program Updates

Before You Begin

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:

© Copyright IBM Corp. 1996

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.

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 RS/6000 SP 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. (See the *SP Commands and Technical Reference* for **spbootins** command syntax.)

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. (See the *SP Commands and Technical Reference* for **splstdata** command syntax.)

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 183.

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.

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. See the *SP Commands and Technical Reference* for more information on **kinit**.

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 /etc/umount /mnt
dsh -a /etc/mount <cw>:/spdata/sys1/install/pssplpp /mnt
dsh -a /etc/installp -d /mnt/ssp/pssp.installp  -X ssp.jm
```

Installing Updates through Reinstallation

Before You Begin

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 recommends 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 20: Initialize RS/6000 SP Authentication Services" on page 30, you cannot use the control workstation for this purpose. Running the **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.

Test Your Image on a Single Node

After you create your netinstall image, you must test the image. Use **ftp** (remember to use binary mode) or **rcp** to transfer the image to the control workstation. The RS/6000 SP 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-frame 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/install server, this may take some time. You can now use the SP 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 SP 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 SP System

This section outlines a procedure you can follow to install PTFs on your SP system using the procedure described in “Installing Updates on a Per Node Basis” on page 185.

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

Before You Begin

Some PTFs require you apply them to all the nodes in your system. To do this, set up a test AIX 4.1 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:

   ```
   /etc/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

Before You Begin

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 /etc/mount <cw>:/spdata/sys1/install/pssplpp /mnt
   ```

2. Use **dsh** to run the appropriate **installp** command to apply PTFs to all nodes.

   ```
   dsh -a /etc/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

Before You Begin

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 29: Update the State of the Supervisor Microcode” on page 46 for more information.

Task F: Create New mksysb Images

- Create a new **mksysb** backup of the control workstation. The **mksysb** image you created in step &mtask.. 6 on page 189 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, type **perspectives**

Note that many of the installation and migration 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, type **spmon -g**

The following table discusses the most common tasks that you can perform using Perspectives or the System Monitor Graphical User Interface (GUI).

Table 7 (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	**TYPE** spmon -g
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** Window→ Exit

© Copyright IBM Corp. 1996

Table 7 (Page 2 of 4). Performing Common Tasks Using SP Perspectives and the System Monitor GUI

Task	Perspectives	System Monitor GUI
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** node to be displayed **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** node to be displayed **PRESS** Display Node Layout **PRESS** On **SELECT** Power on options

Table 7 (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 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 powerLED and switchResponds status. Each variable is displayed in a separate window.
Verifying node status for one node: hostResponds, powerLED, switchResponds, and 3 digit display	From hardware perspective node notebook **SELECT** a node by double clicking on it. **SELECT** Node Status tab 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 **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
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** View → Global (applies to all subsequent actions taken) This action can also be taken anywhere the View menu bar menu appears.

Table 7 (Page 4 of 4). Performing Common Tasks Using SP Perspectives and the System Monitor GUI

Task	Perspectives	System Monitor GUI
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 (applies to all subsequent actions taken) This action can also be taken anywhere the View menu bar appears.

Note: :

SELECT indicates clicking on an icon or a menu choice.

PRESS indicates a button press.

→ indicates a menu item sequence

Appendix B. Directory Information

Table 8 lists the directories created when you install the RS/6000 SP LPP image.

Table 8 (Page 1 of 2). RS/6000 SP LPP Images Directories

Directory	Contents
/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, etc.
/usr/lpp/ssp/config/admin	User mgmt SMIT stanzas
/usr/lpp/ssp/config/cmi	Cluster setup/management SMIT stanzas
/usr/lpp/ssp/config/msg	Message catalogs
/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/backup	Backup files needed for network booting
/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

© Copyright IBM Corp. 1996

Table 8 (Page 2 of 2). RS/6000 SP LPP Images Directories

Directory	Contents
/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
/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	Node accounting data
/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/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:/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
#
#########################################################################
# 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
```

© Copyright IBM Corp. 1996

```
# 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, servers, 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>
#
# Make this node an NIS server
# note: replace <NIS mastername> with the hostname of your NIS
# master
# note: issue: chmaster -s <node hostname>
# on the NIS master to add this node as an NIS server prior to issuing
# the mkslve command on the node.
#
#mkslave <NIS mastername>
#
# Make this node an NIS client
#
#mkclient
#
###############################################################################
```

```
# 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.images/ssp /mnt
#  [[ -f /mnt/pssp.installp     && installp -ac -X
# -d/mnt/xlf.installp all
#
#  # 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
# and 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**.

```
#!/bin/ksh
#"@(#)96    1.2.1.2    src/ssp/samples/tuning.cust, sysman, ssp_rloc 7/24/96 14:18:12"
#########################################################################
#
# 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
#
#  /usr/sbin/no -o udp_sendspace=32768
```

© Copyright IBM Corp. 1996

```
#
#   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 xiv.

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 206 provides details on additional skill areas that may be important at 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 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. 1996

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 9. 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. 1996

Glossary of Terms and Abbreviations

This glossary includes terms and definitions from:

- The *IBM Dictionary of Computing*, New York: McGraw-Hill, 1994.
- The *American National Standard Dictionary for Information Systems*, ANSI X3.172-1990, copyright 1990 by the American National Standards 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). Copies can 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, Joint Technical Committee 1, of the 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 National Standards Institute, Incorporated), 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 Application Programming Guide for TSO Users* (SC26-4081).

© Copyright IBM Corp. 1996

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.

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

Special Characters

/etc/bootptab.info 49
/spdata/sys1/install/images 26, 121, 133
.info 72
.toc
  updating 26

A

adding 150, 155, 165
  frame 150
  nodes 155
  switch 165
addresses
  information verification 50
AFS
  initializing authentication services 38
AIX 4.1 LPP images
  copying 24, 120, 132
AIX image, working with the basic 8
applying ptfs to the SP system 188
attribute in the SDR, changing the node's install image 9
authentication
  initializing RS/6000 SP authentication services 30
    as the authentication client system 36, 94
    as the primary authentication server 31
    as the secondary authentication server 34
  initializing to use AFS 38
  selecting LPP options 29

B

basic AIX image
  installing 27
  working with the 8
bffcreate command 25, 26, 121
boot processing 5, 10
boot/install servers 56
  as NIM masters, configuring 10
  network boot 70
bootp 9
bootp_response 4, 9, 10
bootpd 9
building an installation image 186

C

changing the node's install image attribute 9
chdev command 76
  configuring Ethernet adapter 18, 119, 131
chfs command
  expanding root file system 23, 120
commands
  bffcreate 25, 26, 121
  chdev 76
    configuring Ethernet adapter 18, 119, 131
  chfs
    expanding root file system 23, 120
  crfs
    creating file systems 22
  cshutdown
    shutting down nodes 123, 136
  CSS_test 79, 178
  dsh 185
  Eannotator 66, 172
  Eclock 69, 175
  Eprimary 68, 174
  Estart 78, 177
  Etopology 67, 173
  install_cw 39, 121, 134
  installp
    installing PSSP 27, 30
  mkdev
    configuring Ethernet adapter 18, 119, 131
    configuring RS-232 lines 16
    configuring RS-232 lines / 118, 130
  mklv
    creating logical volumes 22
  mkvg
    creating a volume group 22
  mount
    mounting file systems 22
  no
    displaying network tunable values 19
  SDR_test 40
  setup_server 61
  spadaptrs 54, 55
  spbootins
    changing an SDR attribute 112
    propagating installation image 188
    specifying alternate installation disks 59
    updating the SDR 111
  spdelfram 154
  spdelnode 159, 164
  spethernt 49
  spframe 43
  sphostnam 56
  sphrdwrad 50
  splsdata
    verifying switch configuration 69
  splstdata 51, 60
    determining boot/install servers 71

© Copyright IBM Corp. 1996

commands *(continued)*
spmon_ctest 45
spmon_itest 40
spsitenv 42
sysman_test 64
verifying NIM servers 75
verifying nodes 78
varyonvg
varying on a volume group 22
config_info 9, 10
config_node 74
configuration
reconfiguring RS/6000 SP
adding a frame 150
adding a switch 165
adding nodes 155
deleting a frame 152
deleting nodes 156
replacing a fixed disk 178
replacing Ethernet adapter 181
replacing I/O planar card 181
replacing nodes with different node 162
replacing nodes with equivalent node 159
configuration information, enter node and 4
configure RS-232 control lines 15, 117, 130
configuring
boot/install servers as NIM masters 10
High Availability Control Workstation 83
the RS/6000 SP system 13
control workstation
completing PSSP installation on 39
connecting frames to 15
interface verification 18, 119, 131
prepare and install the 3
preparing 14
requirements verification 14
setup 61
verification requirements 14
verifying System Manager 63
copying
AIX 4.1 LPP images 24, 120, 132
PSSP images 26, 121, 133
crfs command
creating file systems 22
cshutdown command
shutting down nodes 123, 136
css option, updating 185
CSS_test command 79, 178
css0 10
customization 4, 9
defining 63
post-installation 63

D

defining
NIM masters 6
post-installation customization 63
space for NIM boot images 20
space for SP data 20, 119, 131
deleting 152, 156
frame 152
nodes 156
detailed overview of network installation of a node 9
directories created during installation 194
disk, fixed
replacing 178
documentation xvi
dsh command 185
DTMS 82

E

Eclock command 69, 175
enter node and configuration information 4
entering site environment information 40
environment, site 41
Eprimary command 68, 174
Error Log 82
Error Log 82
Estart command 78, 177
Ethernet adapter
configuration 17, 118, 130
replacing 181
Ethernet addresses, acquiring 49
Etopology command 67, 173
externals, install SP on the nodes 4

F

files
switch topology file 64
finding related installation information 13
first boot customization file (script.cust)
sample file 197
first boot customization file (tuning.cust)
sample file 203
fixed disk
replacing 178
fixed disk, replacing a 179
frame supervisor 178
frames
adding 150
deleting 152
entering information 40
spdelfram command 154
full installation 27

G

graphical user interface xvi

H

hardware Ethernet addresses 49
High Availability Control Workstation, installing and configuring the 83
High Performance Switch
  configuring for nodes 51
  setting up 64
  verifying 78
High Performance Switch clock source
  setting 68
host names, configuring for nodes 55

I

I/O planar card
  replacing 181
IBM Virtual Shared Disk 82
  IBM Virtual Shared Disk 82
if_config 72
install
  the control workstation, prepare and 3
  your SP system, planning to 1
install image attribute in the SDR, changing the node's 9
install SP on the nodes
  (externals) 4
  (internals) 5
install_cw command 39, 121, 134
install_image_name 9
install_info 9, 10
installation
  acquiring hardware Ethernet addresses 49
  adding node information 46
  basic AIX image 27
  configuring Ethernet adapter 17, 118, 130
  configuring initial host names 55
  configuring RS-232 control lines 15, 117, 130
  configuring the RS/6000 SP system 13
  connecting frames to control workstation 15
  copying AIX 4.1 LPP images 24, 120, 132
  copying PSSP images 26, 121, 133
  creating adapter objects 51
  creating frame objects in the SDR 42
  defining post-installation customization 63
  defining space for NIM boot images 20
  defining space for SP data 20, 119, 131
  directories creating during 194
  entering site environment information 40, 41
  finding related information 13
  full installation requirements
    images 29
    PSSP options 27
installation *(continued)*
  initializing authentication 30
  installing on existing RS/6000 SP system 109
  installing PSSP on the control workstation 27
  migrating to PSSP V2R1 from PSSP V1R2 109
  mksysb image 27
  network 4, 9
  network booting optional boot/install servers 70
  network booting RS/6000 SP nodes 75
  network requirements verification 15
  nodes 62
  of a node, detailed overview of network 9
  overview of RS/6000 SP 1
  postinstallation procedures 82
  powering on nodes 62
  preparing the control workstation 14
  PSSP 26
  PSSP complete on control workstation 39
  RS/6000 SP system 13
  setting High Performance Switch clock source for all switches 68
  setting up nodes to be installed 56
  setting up system partitions 69
  setting up the control workstation 61
  setting up the High Performance Switch 64
  SSP 29
  starting the switch 78
  tuning the network adapters 80
  updating root user path 14
  verification
    address information 50
    High Performance Switch 78
    High Performance Switch primary node 67
    node information 62, 76
    node tests 77
    optional boot/install servers 75
    SDR 39
    SP System Monitor 39
    SP System Monitor communication facilities 49
    System Manager 63
  verify control workstation requirements 14
  verifying control workstation interface 18, 119, 131
  verifying frame information 44
  without AIX preinstalled 29
installation images
  building 186
  propagation 187
installation information
  finding 13
installation progress, network 71
installation trace, sample NIM 72
installing
  basic AIX mksysb image 27
  nodes 62
  nodes (NIM clients) 6
  program updates 183

installing *(continued)*
PSSP 26
the RS/6000 SP system 13
your SP system 3
installing and configuring the High Availability Control Workstation 83
installp command 8
installing PSSP 27, 30
internals, install SP on the nodes 5

L

Login Control 82
LPP images
copying AIX 4.1 24, 120, 132

M

machine objects 7
maintenance
installing program updates 183
manual pages for public code xxiii
microcode update process 45
migrating nodes 6
migration
authentication
administrative principal 121, 134
completing PSSP installation 121, 134
control workstation
back up 110, 126
creating system partitions
installation
AIX 4.1 on the control workstation 113, 116, 126, 129
AIX 4.1/PSSP V2R1 in test system partition 123, 136
PSSP on the control workstation 121, 134
installing on existing RS/6000 SP system 109
migrating to PSSP V2R1 from PSSP V1R2 109
preparation
AIX 3.2.5 system partition 111
PSSP migration 112, 114, 126
rebooting
nodes in production system partition 123, 136
restoration
saved files 121, 133
shutting down nodes
testing
PSSP 2.2 123
PSSP V2R1 136
validation
upgraded control workstation 122, 135
verification
control workstation requirements 112, 126
SDR 121, 134
system monitor 121, 134
mkdev command
configuring Ethernet adapter 18, 119, 131
configuring RS-232 lines 16, 118, 130
mklv command
creating logical volumes 22
mksysb image
installing 27
mkvg command
creating a volume group 22
mount command
mounting file systems 22

N

netinstall image testing on a single node 187
network adapters
tuning 80
network boot optional boot/install servers 70
network installation 4, 9
of a node, detailed overview of 9
network installation progress 71
network objects 7
network requirements verification 15
new support
System Partitioning Aid 1
NIM boot images
defining space 20
NIM client
definition 6
installing nodes 6
NIM information, storing 7
NIM installation trace, sample 72
NIM master
configuring boot/install servers 10
definition 5
no command
displaying network tunable values 19
node
and configuration information, enter 4
detailed overview of network installation of a 9
node grouping 2
replacing 159, 162
node information
initial entry 46
node's install image attribute in the SDR, changing the 9
nodes
adding 155
configuring initial host names 55
deleting 156
entering information 40
externals, install SP on the 4
information verification 62
installing 62
internals, install SP on the 5
network boot 75

nodes *(continued)*
NIM clients, installing 6
powering 62
replacing with different 162
replacing with equivalent 159
setting up to be installed 56
software maintenance on down nodes 184
updating 185
verification tests 77
verify information using SP System Monitor 76

O

objects
machine 7
network 7
resource 7
overview of network installation of a node, detailed 9
overview of RS/6000 SP installation 1

P

partition-sensitive subsystems 43
per node
basis updating 185
per-node
update installation 183
perl scripts 208
Perspectives xvi, 1, 191
planning
to install your SP system 1
post-installation customization
defining 63
postinstallation procedures 82
powering on nodes 62
prepare and install the control workstation 3
prepare the control workstations 84
preparing the control workstation 14
print management programs
updating 185
print subsystem
updating 185
printing documentation xvi
problem management 2
processing, boot 5, 10
program update installation 183
propagating an installation image 187
PSSP
installation 27
installing 26
reinstalling 184
PSSP 2.2, what's new in 1
PSSP images 26, 121, 133
copying 26, 121, 133
pssp_script 6, 9, 10
ptfs to the SP system, applying 188

R

reconfiguring a system for use with the SP Switch 169
reinstall update installation 183
reinstallation 185
reinstalling PSSP 184
replacing
an I/O planar card in a node 181
Ethernet microchannel adapter 181
fixed disk 179
I/O planar card 181
replacing a frame supervisor 178
Resource Manager 82
Resource Manager 82
resource objects 7
restoring a control workstation from makesysb image 190
root user path
updating 14
RS-232 control lines
configuring 15, 117, 130
RS/6000 SP Facility
RS/6000 SP installation
directory 26, 121, 133
overview 1
RS/6000 SP system
configuring 13
installing 13

S

SAGE
system administrator descriptions 204
sample files 197, 203
script.cust 197
tuning.cust 203
sample NIM installation trace 72
script.cust 5, 6, 9, 10, 30
sample file 197
SDR
changing the node's install image attribute in the 9
reinitializing 42
verifying 39
SDR_test command 40
selecting a topology file 65
serial adapter 97
service
installing 183
setting High Performance Switch clock source for all switches 68
setting up system partitions 69
setup_authent 8
setup_server 6

setup_server command 61
site environment information 41
  entering 40
software maintenance 183
  installing program updates 183
  updating through reinstallation 185
SP data
  defining space 20, 119, 131
SP on the nodes
  (externals), install 4
  (internals), install 5
SP Switch 169
SP system
  applying ptfs to the 188
  installing your 3
  planning to install your 1
SP System Monitor
  verifying 39
SP System Monitor communication facilities
  verifying 49
spadaptrs command 54, 55
spbootins 4, 5, 6, 9, 10
spbootins command
  changing an SDR attribute 112
  propagating installation image 188
  specifying alternate installation disks 59
  updating the SDR 111
spdelfram command 154
spdelnode command 159, 164
spethernt command 49
spframe command 43
sphostnam command 56
sphrdwrad command 50
spimg 8, 29
splsdata command
  verifying switch configuration 69
splstdata command 51, 60
  determining boot/install servers 71
spmon_ctest command 45
spmon_itest command 40
spsitenv command 42
ssp.basic 6, 10
ssp.clients 10
ssp.css 6, 10
ssp.ha 6, 10
ssp.jm 6, 10
ssp.sysctl 6
ssp.sysman 6, 10
storing NIM information 7
supervisor microcode updates 45
switch
  adding 165
  starting 78
switch configuration, verifying 69
switch topology file 64
  annotating 65
switch topology file *(continued)*
  managing 65
  selecting 65
  storing in the SDR 66, 172
Sysctl 82
  Sysctl 82
sysman_test command 64
  verifying NIM servers 75
  verifying nodes 78
system administration
  SAGE job descriptions 204
System Administrators Guide of USENIX, see SAGE
System Monitor Graphical User Interface xvii, 191
system monitor GUI
  verifying frame information 44
system partitions
  setting up 69

T

tftp 9
thin node
  replacing I/O planar card 181
token ring-bridge gateway, using a 75
topology file, selection 65
trace, sample NIM installation 72
trademarks xi
tunable values 19, 119, 131
tuning
  network adapters 80
  tunable values 19, 119, 131
tuning.cust 5, 6
  sample file 203

U

updating
  on a per node basis 185
  root user path 14
  the css option 185
  the print subsystem 185
updating state of supervisor microcode 45
using a token ring-bridge gateway 75

V

varyonvg command
  varying on a volume group 22
verification
  address information 50
  control workstation interface 18, 119, 131
  High Performance Switch primary node 67
  netinstall image 187
  node information 62, 76
  node tests 77
  optional boot/install servers 75

verification *(continued)*
SDR 39
SP System Monitor 39
SP System Monitor communication facilities 49
System Manager on control workstation 63
verifying control workstation requirements 14

W

wide node
replacing Ethernet adapter 181
working with the basic AIX image 8
Worm 64