AlterPath OnBoard Administrator's Guide

cyclades

Cyclades Corporation
3541 Gateway Boulevard
Fremont, CA 94538 USA
1.888.CYCLADES (292.5233)
1.510.771.6100
1.510.771.6200 (fax)
http://www.cyclades.com

Release Date: February 2006
Part Number: PAC0391

Contents

Before You Begin xxix

Audience xxix
Document Organization xxx
Related Documents xxxii
Typographic and Other Conventions xxxiii
Additional Resources xxxv

Chapter 1: Introduction 1

Overview of OnBoard Features for Administrators 3
Understanding Authentication on the OnBoard 4
Understanding User and Group Configuration Options 9
  Parameters for Configuring Users 10
  Configuring Groups 10
  Tasks for Configuring Users and Groups 11
  Planning Access to Connected Devices 11
Understanding Security Profiles 12
Understanding Services on the OnBoard 17
Telnet on the OnBoard 19
  Configuring Telnet for Users 19
  Configuring SSH or Bidilink Instead of Telnet for OnBoard to Device Connections 20
HTTPS on the OnBoard 23
DHCP on the OnBoard 25
  DHCP Client 25
  DHCP Server 25
  Considerations When Deciding Whether to Use DHCP to Configure Device Addresses 26
  Configuring the DHCP Server 26
SNMP on the OnBoard 30

VPN on the OnBoard 32
VPN Client System Requirements and Limitations 33
Configuring VPN 34
IPSec VPN Connections 35
PPTP VPN Connections 38
Message Logging (With Syslog) on the OnBoard 39
Message Filtering Levels 39
Syslog Servers 40
Tasks for Configuring Syslog Messages 40
Understanding Ethernet Ports on the OnBoard 41
Private Ethernet Ports 41
Public Ethernet Ports 41
Tasks for Configuring Ethernet Ports 42
Understanding Modem Access Through the OnBoards 43
Understanding Power Management Options on the OnBoard 46
IPDU Power Management 46
Service Processor Power Management 47
Tasks for Configuring Power Management 47
Configuring the User's Console Login Menu 48
New Menu Item Example 50
Understanding Routing on the OnBoard 51
Default Route Configuration 51
Host or Network Route Configuration 51
Tasks for Configuring Routes 52
Understanding OnBoard Notifications and Sensor Alarms 52
Understanding Device Configuration 53
Preparing an Addressing Scheme 55
Parameters for Configuring Devices 58
Understanding Private Subnets on the OnBoard 61
Tasks for Configuring IP Addresses 62
Example and Demo Scripts and Application Notes 62
Understanding Data Buffering on the OnBoard 62
Understanding Firewall/Packet Filtering on the OnBoard 63
Chains 64
Rules 64
Add Rule and Edit Rule Options 65

Tasks for Administering Packet Filtering 66
Understanding How Configuration Changes Are Handled 67
Saving Configuration Changes 68
Backing Up Configuration File Changes 68
Restoring Backed Up Configuration Files 69
Restoring Factory Default Configuration Files 69
Configuring Files to Be Backed Up and Restored 70
Task for Restoring Configuration Files 71

Chapter 2: Web Manager Introduction 73

Logging Into the Web Manager 74
Features of Administrator's Screens 77
Overview of Web Manager Menus 79

Chapter 3: Web Manager Wizard 81

Using the Wizard 82
Changing the Administrative User's Password—Wizard 84
Selecting a Security Profile—Wizard 85
Secured 88
Open 89
Custom 90
Configuring Network Interfaces—Wizard 91
Configuring Routes 93
Configuring Failover 94
Configuring Primary and Secondary Ethernet Ports 94
Configuring Private Subnets and Virtual Addresses—Wizard 98
Configuring Private Subnets 99
Configuring a Virtual Network 102
Configuring Devices—Wizard 104
Device Types 105
Command Templates 106
Configuring Regular Users —Wizard 107

Chapter 4: Web Manager "Access" Menu Options 111

"Access" Options Only for Administrative Users 112
Accessing the OnBoard Console 113
Viewing IPDU Status and Managing IPDUs 116
Upgrading AlterPath PM IPDU Software 117

Chapter 5: Web Manager "Settings" Menu Options 125

Options Under "Settings" 126
Configuring the AUX Port for Modem or Power Management 127
  Configuring the AUX Port for IPDU Power Management 128
  Configuring the AUX Port for a Modem 129
Configuring IPDU Power Management 132
  Configuring Over Current Protection for an IPDU 133
  Configuring Users to Manage Power Outlets on a Connected IPDU 135
  Configuring Names and Power Up Intervals for Outlets on a Connected IPDU 137
Configuring PCMCIA Cards 139
  Inserting a PCMCIA Card 140
  Ejecting a PCMCIA Card 141
  Configuring a PCMCIA Card 142
  Configuring a Modem PCMCIA Card 143
  Configuring an Ethernet PCMCIA Card 146
  Configuring a Compact Flash PCMCIA Card 148
Configuring System Date and Time 150
Configuring the Boot File Location 152
  Specifying the Boot File Location 152
  Local Boot Options 153
  Network Boot Options 154
  Boot Fields and Menu Options 155
Configuring an Alternate Help File Location 156

Chapter 6: Web Manager “Config” Menu Options 159

Options Under “Config” 161
Configuring Devices 163
Assigning a Device Type and Command Template 165
Device Types 165
Command Templates 165
Configuring Users and Groups 169
Configuring Users 170
Configuring Groups 173
Configuring Authentication 178
Configuring Authentication Servers 179
Configuring a Kerberos Authentication Server 180
Configuring an LDAP Authentication Server 183
Configuring a NIS Authentication Server 185
Configuring a Radius Authentication Server 186
Configuring an SMB Authentication Server 188
Configuring a TACACS+ Authentication Server 190
Configuring an Authentication Method for the OnBoard 192
Configuring Notifications 194
Configuring SNMP Trap Notifications 195
Configuring Pager Notifications 197
Configuring Email Notifications 199
Configuring Sensor Alarms 201
Configuring a “Syslog Message” Sensor Alarm Action 203
Configuring the “SNMP Trap” Sensor Alarm Action 204
Configuring a “Pager” Sensor Alarm Action 207
Configuring an “Email” Sensor Alarm Action 208
Configuring SNMP 209
Configuring SNMP Information Settings 211
Configuring SNMP for Devices 212
Configuring Device SNMP Settings 213
Configuring SNMP Access Settings 215
Fields and Menu Items for Configuring SNMP for Devices 216
Configuring Logging of System Messages (Syslogs) 219

Syslog Destination 220
Filter Messages by Level 220
Configuring the Event Log Backend 222
Selecting or Configuring a Security Profile 224
Secured 226
Open 227
Custom 228
Configuring the OnBoard's Services 229

Chapter 7: Web Manager "Network" Menu Options 231

Options Under "Network" 232
Configuring Network Interfaces 233
Configuring Routes 235
Configuring Failover 236
Configuring Primary and Secondary Ethernet Ports 236
Configuring Firewall Rules for OnBoard Packet Filtering 239
Adding a Rule 240
Configuring Hosts 242
Configuring Static Routes 244
Configuring VPN Connections 246
Configuring IPSec VPN Connections 247
Configuring PPTP VPN Connections 248
Configuring an Address for System Emails 250
Configuring Private Subnets and Virtual Networks 251
Adding Private Subnets 251
Configuring a Virtual Network (DNAT) 253

Chapter 8: Web Manager "Info" and "Mgmt" Menu Options 257

Options Under "Info" 258
Viewing Status Information About Active Sessions 259
Viewing System Information 260
Viewing Information About Detected Devices 263

Options Under “Mgmt” 265
Backing Up or Restoring Configuration Files 266
Upgrading OnBoard Firmware (Operating System Kernel, Configuration Files, and Applications) 267
Information Needed for Firmware Upgrades 268
Configuration Backups Before Upgrading Firmware 269
Special Considerations if the Last Boot Was a Network Boot . 271
Restarting the OnBoard 274

Chapter 9: Using the cycli Utility 275

Accessing the Command Line 276
`cycli` Utility Overview 277
Execution Modes 277
Command Line Mode 278
Interactive Mode 278
Batch Mode 278
`cycli` Options 279
`cycli` Parameters and Arguments 279
Entering Values With Parameters 281
Entering a Command in Interactive Mode 281
Entering a Command in Command Mode 281
Entering a Command in Batch Mode 282
Autocompletion 284
Example: 285
`cycli` Commands 285
add 285
Example: 287
cd 287
Example: 288
commit 288
delete 288
Example: 289
exit 289
get | show 289
Example: 289

Example: 290
Example: 291
list 291
Example: 292
quit | exit 292
Example: 292
quit! 292
rename 292
Example: 293
revert 293
Example: 293
set 293
Example: 294
shell 294
version 294
Summary of How to Configure the Top Level Parameters 295

Chapter 10: Troubleshooting 303

Connection Methods for Troubleshooting 304
Recovering from root Authentication Failure 304
Restarting the Web Manager 306
Replacing a Boot Image for Troubleshooting 307
Using the create_cf Command When Troubleshooting 307

Appendix A: Advanced Device Configuration 309

OnBoard-specific Tasks for Configuring New Devices 310
Understanding How the OnBoard Manages Communications With Devices 311
Device Type Differences 312
Additional Reasons for Creating Custom Expect Scripts 315
Assigning a Command Template to a New Device 316
Command Templates 321
Issues Affecting the Configuration of RSA-Type Service Processors 325

The onbdtemplate Utility 325
OnBoard Expect Scripts 329
Application Notes Related to Expect Scripts 331
Example of Creating a Custom IPMI-Type Script 332
SP/Device Expect Script Arguments 333
servername 333
action 334
SP/Device Expect Script Exit Codes 335
Understanding Address Configuration for Connected Devices 336
Using Reserved IP Addresses for Private IP Addressing 338
Why Define Private Subnets? 339
Configuring a Private Subnet 340
Routing Requirements for Native IP Access 341
Example 1: Private Subnet Configuration 342
Example 2: Two Private Subnets and VPN Configuration 345
Two Private Subnets and User Configuration for Example 2 ... 346
IPSec VPN Configuration for Example 2 349
PPTP VPN Configuration for Example 2 352
Enabling Native IP and Accessing a Device's Native Features Using Real IP Addresses for Example 2 355
Why Define Virtual (DNAT) Addresses? 357
Example 3: Virtual Network With Two Private Subnets and VPN Configuration 358
Virtual Network and Device Configuration for Example 3 360
IPSec VPN Configuration for Example 3 362
PPTP VPN Configuration for Example 3 364
Enabling Native IP and Accessing a Device's Native Features Using Virtual Network Addresses for Example 3 365
Options for Assigning IP Addresses to Connected Devices 368
Additional Network Address Configuration Examples 368

Appendix B: Advanced Boot and Backup Configuration Information..... 371

Boot File Location Information 372
Downloading a New Software Version 374

Changing the Boot Image 375
Changing the Boot Image in U-Boot Monitor Mode 376
Network Boot Options and Caveats 378
Options for the create_cf Command 381
Examples for create_cf Command Usage 383
Saving an Image to a Flash PCMCIA Card 383
Saving an Image into the Image2 area and Restoring the Factory Default Configuration. 383
Options for the restoreconf Command 384

Glossary 385

Index 411

Figures

Figure 1-1: Default `/etc/menu.ini` File 48
Figure 1-2: Example: Onetime Password Option Added to `menu.ini50`
Figure 1-3: Recommended Device Configuration 55
Figure 1-4: IP Addressing Example 57
Figure 2-1: Web Manager Message When An Administrative User is Already Logged In 75
Figure 2-2: Administrative User Options on the Web Manager 77
Figure 2-3: Example Dialog: Devices Configuration—in Wizard ... Mode 79
Figure 3-1: Wizard Screen 82
Figure 3-2: “Cancel Wizard” Button Dialog 83
Figure 3-3: Wizard “Confirm Changes” Screen 83
Figure 3-4: Wizard “Configure Administrator Password” Screen 84
Figure 3-5: Config → Security Profile Screen With the “Moderate” Profile Enabled 86
Figure 3-6: Security Profile Configuration Dialog With “Moderate” Profile Selected 86
Figure 3-7: Security Profile Confirmation Screen 87
Figure 3-8: Secured Profile Dialog 88
Figure 3-9: Open Security Profile Dialog 89
Figure 3-10: Custom Security Profile Dialog 90
Figure 3-11: Network Interfaces Screen—Wizard 91
Figure 3-12: “Configure Failover Device” Screen 94
Figure 3-13: “Configure Primary Ethernet Connection” Screen 95

Figure 3-14: "Configure Primary Ethernet Connection:" Enabled With DHCP 95
Figure 3-15: "Configure Primary Ethernet Connection" Screen: Static IP 96
Figure 3-16: "Configure Subnets" Screen—Wizard 98
Figure 3-17: "Configure Subnets" Screen—Wizard: Add Subnet Dialog 99
Figure 3-18: Network → Private Subnets: Add Subnet Dialog 100
Figure 3-19: "Configure Subnets" Screen: Virtual Network (DNAT) Configuration 102
Figure 3-20: "Configure Devices" Screen—Wizard 104
Figure 3-21: "Add New Device" Dialog—Wizard 105
Figure 3-22: "Add a Regular User" Screen—Wizard 107
Figure 4-1: Access Menu Options 112
Figure 4-2: Administrative User Console Session Window—Initial Connection from an IP Address 113
Figure 4-3: OnBoard Console Login Dialog 114
Figure 4-4: OnBoard Console Login Prompt for Administrative Users 114
Figure 4-5: Tabs Under Access → IPDU 116
Figure 4-6: IPDU "Software Upgrade" Screen 117
Figure 4-7: Upgrade Button on the IPDU "Software Upgrade" Screen 118
Figure 4-8: IPDU Software Upgrade Dialog 118
Figure 4-9: IPDU "Software Upgrade" Screen With Upgraded Software 119
Figure 5-1: "Settings" Menu Options 126
Figure 5-2: Settings → Aux Port Screen 127
Figure 5-3: Settings → AUX Port → Power Management 128
Figure 5-4: Settings → AUX Port → Modem 129
Figure 5-5: Settings → AUX Port → Modem 130

Figure 5-6: Callback Number Field Under Settings → AUX Port → Modem 130
Figure 5-7: Settings → AUX Port → Modem 131
Figure 5-8: Settings → IPDU Screen 132
Figure 5-9: Settings → IPDU Screen Without AUX Port Configuration 132
Figure 5-10: Settings IPDU General Screen 133
Figure 5-11: Settings IPDU General Screen 134
Figure 5-12: Edit Alarm Threshold for IPDU Dialog 134
Figure 5-13: Settings → IPDU → Users Screen 136
Figure 5-14: Settings → IPDU → Users → Add User Dialog 136
Figure 5-15: Settings → IPDU → Users With a User Added 136
Figure 5-16: Settings → IPDU → Outlets Screen 138
Figure 5-17: Outlet Name Dialog 138
Figure 5-18: Outlet Power Up Interval Dialog 138
Figure 5-19: Settings → PCMCIA Screen 139
Figure 5-20: Insert PCMCIA Query 140
Figure 5-21: Example: PCMCIA Ethernet Card inserted in Slot 1 141
Figure 5-22: Eject PCMCIA Dialog 141
Figure 5-23: Settings → PCMCIA → Configure Modem Dialog 143
Figure 5-24: Settings → PCMCIA → Configure Modem Callback 144
Figure 5-25: Settings → PCMCIA → Configure Modem → Login 144
Figure 5-26: Settings → PCMCIA → Configure Modem → PPP 145
Figure 5-27: Settings → PCMCIA → Configure Ethernet Dialog 147
Figure 5-28: Settings → PCMCIA → Configure Ethernet Dialog Without DHCP 147

Figure 5-29: Settings → PCMCIA → Configure Compact Flash Dialog: Mount Option Unchecked 148
Figure 5-30: Settings → PCMCIA → Configure Compact Flash Dialog 149
Figure 5-31: Settings → Date/time Screen 150
Figure 5-32: Settings → Date/time Screen: Timezone Pull-down 150
Figure 5-33: Settings → Date/time Screen With NTP Fields 151
Figure 5-34: Settings → Date/time Screen 151
Figure 5-35: Settings → Boot Configuration Screen 152
Figure 5-36: Settings → Boot Configuration → Unit Boot Menu 153
Figure 5-37: Settings → Help Screen 156
Figure 6-1: "Config" Menu Options 161
Figure 6-2: Config → Devices Screen 163
Figure 6-3: Fields in the "Add New Device" or "Edit" Dialog ... 164
Figure 6-4: Config → Users and Groups Screen 169
Figure 6-5: Add New User or Edit Dialog 170
Figure 6-6: Add or Edit a User's Device Access Dialog 171
Figure 6-7: Add New Device or Edit Device Dialog 172
Figure 6-8: Add New Group or Edit Dialog 173
Figure 6-9: Group Configuration Buttons 173
Figure 6-10: Add or Edit a Group's Device Access Dialog 174
Figure 6-11: Add New Device to a Group Dialog 174
Figure 6-12: Default Config → Authentication Screen 179
Figure 6-13: Config → Authentication: Kerberos 180
Figure 6-14: Config → Authentication: LDAP 183
Figure 6-15: Config → Authentication: NIS 185
Figure 6-16: Config → Authentication: Radius 186
Figure 6-17: Config → Authentication: SMB 188
Figure 6-18: Config → Authentication: TACACS+ 190

Figure 6-19: Default Config → Authentication Screen 192
Figure 6-20: Default Config → Unit Authentication Screen With Menu Options 193
Figure 6-21: Default Config → Notifications Screen 194
Figure 6-22: Config → Notifications: SNMP Trap Add Dialog.... 195
Figure 6-23: Config → Notifications: Pager Add Dialog 197
Figure 6-24: Default Config → Notifications: Email Add Dialog 199
Figure 6-25: Default Config → Sensor Alarms Screen 201
Figure 6-26: Default Config → Sensor Alarms Screen 201
Figure 6-27: Config → Sensor Alarms Syslog Message Fields 203
Figure 6-28: Config → Sensor Alarms SNMP Trap Fields 205
Figure 6-29: Config → Sensor Alarms Pager Message Fields 207
Figure 6-30: Config → Sensor Alarms Email Message Fields..... 208
Figure 6-31: Config → SNMP Configuration Screen 210
Figure 6-32: Config → SNMP: Edit OnBoard Information Settings 211
Figure 6-33: Config → SNMP: SNMP Configure Dialog..... 212
Figure 6-34: Device SNMP Settings Screen..... 212
Figure 6-35: Config → SNMP: Device SNMP Access Dialog With V1 Selected 213
Figure 6-36: Config → SNMP: Device SNMP Access Dialog With V2c Selected..... 214
Figure 6-37: Config → SNMP: Device SNMP Access Dialog With V3 Selected 214
Figure 6-38: Config → SNMP: Device SNMP Access Dialog With V1 Selected 215
Figure 6-39: Config → Device SNMP Settings Dialog With V2c Selected..... 215
Figure 6-40: Config → Device SNMP Settings Dialog With V3 Selected 216
Figure 6-41: Config → Syslog Screen..... 219

Figure 6-42: Config → Event Log Backend Screen 222
Figure 6-43: Config → Event Log Backend: Edit Dialog 222
Figure 6-44: Config → Security profile Screen 224
Figure 6-45: Config → Security Profile Dialog With the "Moderate" Profile Enabled 225
Figure 6-46: Config → Security Profile Dialog With the "Secured" Profile Enabled 226
Figure 6-47: "Open" Security Profile Dialog 227
Figure 6-48: "Custom" Security Profile Dialog 228
Figure 6-49: Config → Services Screen 229
Figure 7-1: "Network" Menu Options 232
Figure 7-2: Network → Host Settings Screen 233
Figure 7-3: Network → Host Settings Screen With Failover Enabled 236
Figure 7-4: Network → Host Settings Screen With Both Interfaces Enabled and DHCP Disabled 237
Figure 7-5: Network → Firewall Screen 239
Figure 7-6: Network → Firewall: Add Rule Dialog 240
Figure 7-7: Network → Host Table Screen 242
Figure 7-8: Network → Host Table: Add New Host Dialog 243
Figure 7-9: Network → Static Routes Screen 244
Figure 7-10: Network → Add New Static Route Dialog 244
Figure 7-11: Network → VPN Connections Screen 246
Figure 7-12: IPSec VPN Connection Configuration Dialog 247
Figure 7-13: PPTP VPN Connection Configuration Fields 249
Figure 7-14: Network → Outbound Email Screen 250
Figure 7-15: Network → Private Subnets Screen 251
Figure 7-16: Network → Private Subnets: Add Subnet Dialog 252
Figure 7-17: Network → Private Subnets: Add Subnet Dialog 253
Figure 7-18: Network → Private Subnets: Virtual Network Configuration Fields 254

Figure 8-1: "Info" Menu Options 258
Figure 8-2: Info → Session Status Screen 259
Figure 8-3: Info → System Information Screen 260
Figure 8-4: Info → Detected Devices Screen 263
Figure 8-5: "Mgmt" Options 265
Figure 8-6: Mgmt → Backup/Restore Screen 266
Figure 8-7: Mgmt → Firmware Upgrade Screen 267
Figure 8-8: Mgmt → Firmware Upgrade Screen With Net Boot Message 271
Figure 8-9: Mgmt → Restart Screen 274
Figure 9-1: Example Branch in the `cycli` Parameter Tree 280
Figure A-1: `onboard_server.ini` Device Entries With Templates Assigned 324
Figure A-2: Example 1: Private Subnet 342
Figure A-3: Private Subnet Configuration Example 343
Figure A-4: Example 1: Device Configuration Example 344
Figure A-5: `ifconfig` Output Showing a `priv0` Private Subnet Alias 344
Figure A-6: Example 2: Two Private Subnets 345
Figure A-7: Example 2: Values for Configuring Two Subnets on the Network → Private Subnet Screen 346
Figure A-8: `ifconfig` Output With `priv0` Aliases for Two Private Subnets 347
Figure A-9: Example 2: Four Devices Configured on the Web Manager Config → Devices Screen 348
Figure A-10: Example 2: Configuration for a User Account Authorized for Native IP Access to All Configured Devices 348
Figure A-11: Example 2: IPSec Connection Configuration for Access to sub1 Private Subnet and "sp1" and "sp2" Devices 351
Figure A-12: PPTP VPN Configuration Example: Address Pools . 352

Figure A-13: PPTP User Configuration Example 353
Figure A-14: Example 3: Virtual Network Configuration 359
Figure A-15: Example Values for Configuring Two Private Subnets With a Virtual Network 360
Figure A-16: Example 1: Device Configuration Example 361
Figure A-17: Access → Devices Screen With Virtual IP Addresses 362
Figure A-18: Example 3: IPSec Connection Configuration for Access to sub1 Private Subnet and “sp1” and “sp2” Devices 363
Figure B-1: Boot Partitions 373

Tables

Table P-1: Document Organization xxx
Table P-2: Related Documentation xxxii
Table P-3: Typographic Conventions xxxiii
Table P-4: Other Terms and Conventions xxxiv
Table 1-1: Security Features and Where Documented 3
Table 1-2: Supported Authentication Types 5
Table 1-3: Tasks for Configuring Authentication 8
Table 1-4: User Configuration Settings 10
Table 1-5: Tasks for Configuring Users and Groups. 11
Table 1-6: Moderate Security Profile Services/ Features 12
Table 1-7: Secured Security Profile Services/Features 13
Table 1-8: Open Security Profile Services/Features 13
Table 1-9: Services and Other Functions in the "Custom" Security Profile 14
Table 1-10: Services That Require Additional Configuration 17
Table 1-11: Tasks for Changing the Default telnet Configuration . 19
Table 1-12: Required Information When Creating a SSL Certificate Request 23
Table 1-13: Tasks for Configuring SNMP 31
Table 1-14: VPN Client System Requirements and Limitations 33
Table 1-15: Tasks for Configuring VPN Connections 34
Table 1-16: IPSec VPN Configuration Information for Administrators and Users 35
Table 1-17: Tasks for Configuring Syslog Messages 40
Table 1-18: Tasks for Configuring Ethernet Ports 42
Table 1-19: Tasks for Configuring and Installing Modems 43
Table 1-20: Modem Configuration Field and Menu Definitions ... 44

Table 1-21: Tasks for Configuring Power Management 47
Table 1-22: Example: Option Added to Menu for Regular Users.. 50
Table 1-23: Tasks for Configuring Routes 52
Table 1-24: Device Configuration Parameters 58
Table 1-25: Filter Options for Packet Filtering Rules 65
Table 1-26: Tasks for Configuring Packet Filtering (Firewall) Rules..... 66
Table 1-27: Options for Saving Configuration File Changes..... 68
Table 1-28: Options for Saving Configuration File Changes..... 68
Table 1-29: Options for Saving Configuration File Changes..... 69
Table 1-30: Options for Saving Configuration File Changes..... 69
Table 2-1: Buttons That Display Only for Administrative Users..... 78
Table 3-1: Wizard Steps and Where They are Described..... 84
Table 3-2: Network Interfaces Configuration Values..... 92
Table 3-3: Ethernet Port Settings..... 93
Table 3-4: Fields on the Private Subnet Configuration Dialog .. 100
Table 3-5: Fields on the Private Subnet Virtual Network Configuration Dialog..... 103
Table 3-6: Default Command Templates..... 106
Table 3-7: User Configuration Settings..... 107
Table 4-1: Tasks for Upgrading Software on a Connected IPDU 119
Table 5-1: Options Under Settings 126
Table 5-2: Options Under Settings → IPDU 133
Table 5-3: PCMCIA Action Buttons..... 140
Table 5-4: Boot Configuration Fields and Options 155
Table 6-1: Options Under “Config” 161
Table 6-2: Default Command Templates..... 166
Table 6-3: User Configuration Settings..... 170
Table 6-4: Tasks for Authentication Configuration..... 178
Table 6-5: Fields for Configuring an SNMP Trap Notification . 195

Table 6-6: Fields for Configuring a Pager Notification 198
Table 6-7: Fields for Configuring an Email Notification 199
Table 6-8: Fields for Configuring Sensor Alarms 202
Table 6-9: Fields for Configuring Syslog Message Sensor Alarms 204
Table 6-10: Fields for Configuring a SNMP Trap Sensor Alarms 205
Table 6-11: Fields for Configuring Syslog Message Sensor Alarms 207
Table 6-12: Fields for Configuring Email Sensor Alarms 209
Table 6-13: Tasks for Configuring SNMP 210
Table 6-14: Fields for Configuring SNMP 216
Table 7-1: Options Under “Network” 233
Table 7-2: Network Interfaces Configuration Values 234
Table 7-3: Fields and Menus for Configuring Static Routes 245
Table 7-4: Fields for Configuring a PPTP Profile 249
Table 7-5: Fields on the Private Subnet Configuration Dialog .. 252
Table 7-6: Fields on the Private Subnet Virtual Network Configuration Dialog 254
Table 8-1: Options Under Info 258
Table 8-2: Information on the Info → Session Status Screen 259
Table 8-3: Information on the System Information Screen 261
Table 8-4: Information on the Info → Detected Devices Screen 263
Table 8-5: Tasks Performed Under the Web Manager “Mgmt” Tab 265
Table 8-6: Firmware Upgrade Screen Fields 268
Table 9-1: `cycli` Utility Options 279
Table 9-2: Top Level `cycli` Parameters With Set or Add Commands 295
Table A-1: OnBoard-specific Tasks for Configuring New Devices 310
Table A-2: Device Type Differences 313

Table A-3: Reasons for Customizing Expect Scripts 315
Table A-4: Default Command Templates..... 321
Table A-5: Default Device Types and Corresponding Expect Scripts..... 329
Table A-6: Custom Device Types and Corresponding Expect Scripts..... 329
Table A-7: Expect Script Related Application Notes..... 331
Table A-8: Expect Script Exit Codes 335
Table A-9: Tasks for Creating Addresses to Assign to Connected Devices..... 336
Table A-10: IP Address Ranges Reserved for Internal Network Addressing..... 338
Table A-11: Values for Configuring a Private Subnet..... 341
Table A-12: Examples for Creating IPSec and PPTP VPN Connections for Example 2..... 349
Table A-13: Information Defining a Virtual (DNAT) Network 358
Table B-1: Options for the create_cf command 382

Procedures

Chapter 1: Introduction 1

- To Substitute SSH or bidilink for Telnet for Device Connections 20
- To Replace the Self-Signed Certificate With an SSL Certificate From a Certificate Authority 23
- To Configure DHCP for Managing IP Addresses of Connected Devices 27
- To Modify the Menu Displayed for Users at Console Login 51
- To Configure an Added Script or Other File for Backup and Restoration 70

Chapter 2: Web Manager Introduction 73

- To Log Into the Web Manager 75
- To Disable Web Manager Timeouts 76

Chapter 3: Web Manager Wizard 81

- To Change the Administrative User's Password—Wizard 85
- To Select or Configure a Security Profile—Wizard 91
- To Configure OnBoard Network Interfaces—Wizard 96
- To Add a Private Subnet—Wizard 101
- To Edit a Private Subnet—Wizard 101
- To Configure a Private Subnet and Optional Virtual Network—Wizard 103
- To Create and Authorize a User for Device Management—Wizard 108

Chapter 4: Web Manager "Access" Menu Options 111

- To Access the OnBoard's Console 115
- To Download AlterPath PM IPDU Software From Cyclades 119

▼ To Upgrade Software on a Connected IPDU 122

Chapter 5: Web Manager “Settings” Menu Options 125

▼ To Configure an AUX Port for IPDU Power Management 128
▼ To Configure an AUX Port for Modem Access 131
▼ To Enable Overcurrent Protection for an AlterPath PM IPDU 135
▼ To Configure a User to Manage Power Outlets on a Connected IPDU 137
▼ To Configure an Alias and a Power Up Interval for an IPDU Outlet 138
▼ To Begin Configuring a PCMCIA Card 142
▼ To Configure a Modem PCMCIA Card 145
▼ To Configure an Ethernet PCMCIA Card 147
▼ To Configure a Compact Flash PCMCIA Card 149
▼ To Configure System Date and Time 151
▼ To Configure OnBoard Boot 155
▼ To Specify a New Location for OnBoard Help Files 157

Chapter 6: Web Manager “Config” Menu Options 159

▼ To Add a Device 166
▼ To Sort the Device List Alphabetically 168
▼ To Create and Authorize a User for Device Management 174
▼ To Modify a User’s Account 175
▼ To Create and Authorize a Group for Device Management 177
▼ To Configure a Kerberos Authentication Server 181
▼ To Configure an LDAP Authentication Server 184
▼ To Configure a NIS Authentication Server 185
▼ To Configure a Radius Authentication Server 187
▼ To Configure an SMB Authentication Server 189
▼ To Configure a TACACS+ Authentication Server 191
▼ To Configure an Authentication Method for OnBoard Logins 193
▼ To Configure SNMP Trap Notifications 196

▼ To Configure Pager Notifications 198
▼ To Configure an Email Notification 200
▼ To Begin Configuring a Sensor Alarm 202
▼ To Configure a Syslog Message Sensor Alarm Action 204
▼ To Configure an SNMP Trap Sensor Alarm Action 206
▼ To Configure a Pager Sensor Alarm Action 208
▼ To Configure an Email Sensor Alarm Action 209
▼ To Configure OnBoard SNMP Information 211
▼ To Configure SNMP for a Device 217
▼ To Configure the Syslog Destination and Message Filtering 221
▼ To Configure Event Logging for Connected Service Processors 223
▼ To Select the OnBoard's Security Profile 229
▼ To Configure Services 230

Chapter 7: Web Manager "Network" Menu Options 231

▼ To Configure OnBoard Network Interfaces 237
▼ To Add a New Packet Filtering (Firewall) Rule 241
▼ To Edit an Administrator-added Packet Filtering (Firewall) Rule 241
▼ To Add a New Host 243
▼ To Add a Static Route 245
▼ To Configure IPSec VPN 247
▼ To Configure a PPTP VPN Connection 249
▼ To Configure Outbound Email 250
▼ To Configure a Private Subnet 254
▼ To Configure a Virtual Network 255

Chapter 8: Web Manager "Info" and "Mgmt" Menu Options 257

▼ To Back Up Configuration Files 267
▼ To Restore Backed-up Configuration Files 267
▼ To Download OnBoard Firmware From Cyclades 269

▼ To Upgrade the OnBoard's Operating System, Applications, and Configuration Files 272
▼ To Restart the OnBoard 274

Chapter 10: Troubleshooting 303

▼ To Recover from root Authentication Failure 305
▼ To Restart the Web Manager 306

Appendix A: Advanced Device Configuration ... 309

▼ To Find Out if An Existing Command Template Works With a New Device 317
▼ To Use the onbdtemplate Utility to Create a New Template 318
▼ To Use the onbdtemplate Utility to Test a Template 320
▼ To Create a Custom IPMI Expect Script 333
▼ To Create a Custom Expect Script 336

Advanced B: Boot and Backup Configuration Information 371

▼ To Boot from an Alternate Image Using cycli 375
▼ To Boot in U-Boot Monitor Mode 377
▼ To Boot from an Alternate Image in U-Boot Monitor Mode 377
▼ To Boot in Single User Mode from U-Boot Monitor Mode 378
▼ To Replace a Boot Image From a Network Boot in U-Boot Monitor Mode 379
▼ To Restore the OnBoard Configuration Files to the Last Saved Version 380
▼ To Restore the OnBoard Configuration Files to the Factory Defaults 381

Before You Begin

This *AlterPath OnBoard Administrator's Guide* provides information and procedures for configuring and managing the Cyclades™ AlterPath™ OnBoard. It describes what the administrator needs to know and to do in order to securely control access to management services provided by connected service processors and other connected servers and devices that allow access to their consoles through Ethernet ports.

Audience

This manual is intended for system administrators of the OnBoard. The *AlterPath OnBoard Administrator's Guide* is for administrators who are authorized to configure access to service processors and other devices connected to the OnBoard during installation. (For installation details, see the *AlterPath OnBoard Installation Guide*.)

This document describes configuration and administration of the OnBoard only. It does not describe how to set up and administer other external services or servers that the OnBoard may access for authentication, system logging, IPMI control, SNMP notifications, data logging, file sharing, or other purposes. This document assumes that users who are authorized to access server-management services on connected servers already know understand the services provided and how to use them to manage the connected devices.

Document Organization

The document contains the chapters listed in the following table.

Table P-1: Document Organization

Chapter Number and Title	Description
1: Introduction	Describes what OnBoard administrators need to know in order to perform configuration and maintenance tasks while enforcing the organization's security policies.
2: Web Manager Introduction	Provides an overview of all the Web Manager features and menu options that are available for administrative users. Also provide procedures for logging into the Web Manager and for disabling timeouts.
3: Web Manager Wizard	Describes and provides procedures for how the administrative user uses the Web Manager Wizard to perform basic configuration
4: Web Manager "Access" Menu Options	Describes and provides procedures for how to use the Web Manager menu options that are available to administrative users under the "Access" top menu option.
5: Web Manager "Settings" Menu Options	Describes and provides procedures for how to use the Web Manager menu options that are available to administrative users under the "Settings" top menu option.
6: Web Manager "Config" Menu Options	Describes and provides procedures for how to use the Web Manager menu options that are available to administrative users under the "Config" top menu option.

Table P-1: Document Organization (Continued)

Chapter Number and Title	Description
7: Web Manager "Network" Menu Options	Describes and provides procedures for how to use the Web Manager menu options that are available to administrative users under the "Network" top menu option.
8: Web Manager "Info" and "Mgmt" Menu Options	Describes and provides procedures for how to use the Web Manager menu options that are available to administrative users under the "Info" and "Mgmt" top menu options.
9: Using the cycli Utility	Describes how an administrator can access the Linux command line on the AlterPath OnBoard and can use the `cycli` utility.
6: Troubleshooting	Provides troubleshooting procedures.
A: Advanced Device Configuration	Describes and provides advanced procedures for configuring a new device
B: Advanced Boot and Backup Configuration Information	Describes and provides procedures for configuring the boot file location and managing configuration file changes.
Glossary	Defines terms used in Cyclades product documents.
Index	Provides a way to look up terms. In the online version of this manual, clicking the terms in the index brings you to where they are used in the manual.

Related Documents

The following table lists the AlterPath OnBoard documents. As indicated, the QuickStart Guide is printed, and it is also included with the other AlterPath OnBoard documents in PDF format on the Documentation CD that is shipped with the product. The documents are also at http://www.cyclades.com/docs under "AlterPath OnBoard."

Table P-2: Related Documentation

Guide Title	Printed and Shipped?	PDFs on DocCD?	Part Number
AlterPath OnBoard QuickStart Guide	Y	Y	PAC0389
AlterPath OnBoard Installation Guide	N (may be ordered separately)	Y	PAC0390
AlterPath OnBoard User's Guide	N (may be ordered separately)	Y	PAC0392

Before installing or using this product, refer to the release notes for important information about supported hardware and software, known problems, and outstanding bugs. You can download the release notes by going to `http://www.cyclades.com/support/downloads.php` and searching for the product name "AlterPath OnBoard."

The OnBoard has been tested with specific models of devices and firmware levels that are also listed in the release notes. Before configuring a device, check the release notes to ensure that both the device you want to connect to the OnBoard and its firmware level are listed, and if the device model and firmware version is not listed in the release notes, refer to Appendix A, 'Advanced Device Configuration" on page 309," for how to configure the device.

The OnBoard also ships with application notes that are in `/usr/share/docs/OnBoard/Application_Notes`. Check for updated application notes also at `http://www.cyclades.com/support/downloads.php` under the product name "AlterPath OnBoard."

Printed versions of this document and all the above listed documents can be ordered from a Cyclades sales representative.

Documents for the AlterPath PM mentioned in this guide are also on the Documentation CD shipped with the product, and they are also available at: http://www.cyclades.com/support/downloads.php under the product's name.

Updated versions of this document will be posted at the Cyclades website when Cyclades releases new versions of the software. See "Additional Resources" on page xxxv for information about free software upgrades.

Typographic and Other Conventions

The following table describes the typographic conventions used in Cyclades manuals.

Table P-3: Typographic Conventions

Typeface	Meaning	Example
Links	Hypertext links or URLs	Go to: http://www.cyclades.com
Emphasis	Titles, emphasized or new words or terms	See the *AlterPath OnBoard Quick Start.*
`Filename or Command`	Names of commands, files, and directories; onscreen computer output.	Edit the `pslave.conf` file.
`User type`	What you type in an example, compared to what the computer displays	[root] **`ifconfig eth0`**

The following table describes other terms and conventions.

Table P-4: Other Terms and Conventions

Term or Convention	Meaning	Examples
Hot keys	When hot keys are shown, a plus (+) appears between two keys that must be pressed at the same time, and a space appears between two keys that must be pressed sequentially.	• `Ctrl+k p` entered while the user is connected to a KVM port brings up an IPDU power management screen. `Ctrl` and `k` must be pressed at the same time followed by `p` pressed by itself. • `Ctrl+Shift+i` entered while the user is connected to a serial port brings up the IPMI power management utility. The `Ctrl` key and the `Shift` and `i` keys must be pressed at the same time.
Navigation shortcuts	Shortcuts use the → symbol to indicate how to navigate to Web Manager forms or OSD screens.	Go to Configuration → KVM → General → IP Users in Expert mode.

Additional Resources

The following sections describe how to get technical support, training, and software upgrades.

Cyclades Technical Support

Cyclades offers free technical support. To find out how to contact the support center in your region, go to: http://www.cyclades.com/support/technical_support.php.

Cyclades Technical Training

To learn about Cyclades Technical Training Center and courses offered, visit http:www.cyclades.com/training, call 1-888-292-5233, or send an email to training@cyclades.com.

Cyclades Software Upgrades

Cyclades offers periodic software upgrades for the AlterPath products free of charge to current Cyclades customers. You may want to check http://www.cyclades.com/support/downloads.php from time to time to see if upgrades are available for the OnBoard or for an AlterPath PM or AlterPath KVM Terminators that you may also be using with this product.

See “To Upgrade the OnBoard’s Operating System, Applications, and Configuration Files” on page 272 for instructions on upgrading the software on your AlterPath OnBoard. See also “To Upgrade Software on a Connected IPDU” on page 122 for how to upgrade the software on any connected AlterPath PM IPDUs.

Chapter 1
Introduction

The administrator configures the OnBoard to enable controlled access to connected devices and also performs maintenance activities such as upgrading the OnBoard software. This chapter describes what OnBoard administrators need to know in order to perform configuration and maintenance tasks while enforcing the organization's security policies.

The *AlterPath OnBoard User's Guide* is prerequisite reading for understanding the information and procedures in this chapter and in other chapters in this administrator's guide.

The following table lists the topics in this chapter.

Overview of OnBoard Features for Administrators	Page 3
Understanding Authentication on the OnBoard	Page 4
Understanding User and Group Configuration Options	Page 9
Understanding Security Profiles	Page 12
Understanding Services on the OnBoard	Page 17
Telnet on the OnBoard	Page 19
HTTPS on the OnBoard	Page 23
DHCP on the OnBoard	Page 25
SNMP on the OnBoard	Page 30
VPN on the OnBoard	Page 32
Message Logging (With Syslog) on the OnBoard	Page 39
Understanding Ethernet Ports on the OnBoard	Page 41
Understanding Modem Access Through the OnBoards	Page 43
Understanding Power Management Options on the OnBoard	Page 46

Configuring the User's Console Login Menu	Page 48
Understanding Routing on the OnBoard	Page 51
Understanding OnBoard Notifications and Sensor Alarms	Page 52
Understanding Device Configuration	Page 53
Understanding Private Subnets on the OnBoard	Page 61
Tasks for Configuring IP Addresses	Page 62
Example and Demo Scripts and Application Notes	Page 62
Understanding Data Buffering on the OnBoard	Page 62
Understanding Firewall/Packet Filtering on the OnBoard	Page 63
Understanding How Configuration Changes Are Handled	Page 67

Overview of OnBoard Features for Administrators

The OnBoard mediates between *authorized users* (who may be either local or remote users on the *public network*) and devices that are connected to the OnBoard's private Ethernet ports. Connected devices are almost always isolated on a *private network* that cannot be accessed except by going through the OnBoard.

Communications between users and the OnBoard and through the OnBoard to connected devices are protected by SSH encryption. Communications between the OnBoard and the connected devices are proxied and the potentially vulnerable *protocols* used by most service processors are not exposed on the public network.

Administration of the OnBoard is separate from management of the connected devices: multiple authorized users can manage connected devices while only OnBoard administrators can configure access and security on the OnBoard.

The OnBoard provides a set of security features not available in any service processor management product from any other vendor. The following table lists the features that OnBoard administrators can configure to control access to connected devices and to enforce an organization's security policies and lists where the features are documented in more detail.

Table 1-1: Security Features and Where Documented

Security Feature	Where Documented
Authentication for accessing the OnBoard and connected devices	"Understanding Authentication on the OnBoard" on page 4
Authorizations assigned to users and groups to control access to connected devices	"Types of Users" and "Types of User Authorizations" in *AlterPath OnBoard User's Guide*
Security profiles and other means for controlling which network services are turned on or blocked and for setting other security parameters	"Understanding Security Profiles" on page 12 "Understanding Services on the OnBoard" on page 17

Table 1-1: Security Features and Where Documented (Continued)

Security Feature	Where Documented
Logging, *notifications*, and *alarms* that can alert remote administrators about problems, and *data buffering* to capture and monitor user activity.	"Understanding OnBoard Notifications and Sensor Alarms" on page 52 "Configuring Notifications" on page 194 "SNMP on the OnBoard" on page 30 "Understanding Data Buffering on the OnBoard" on page 62 "Understanding Firewall/Packet Filtering on the OnBoard" on page 63

Understanding Authentication on the OnBoard

The OnBoard administrator can select among many common authentication types for the following types of logins:

- For logins to the OnBoard
- For logins to connected devices

By default, all logins to the OnBoard and connected devices use Local authentication. Administrators can specify separate authentication types for OnBoard logins and for connected devices.

Note: This section discusses only the types of authentication used for controlling who can access the OnBoard and connected devices. Other authentication methods that are used by SNMP, PPTP, IPSec, or PPP are described in the related sections.

The following table lists the supported authentication methods and indicates which methods are available for the OnBoard and which are available for connected devices. All authentication methods (except “Local”) require an authentication server. When a table cell is blank, the authentication method is not supported.

Table 1-2: Supported Authentication Types (Sheet 1 of 3)

Type	Description	OnBoard	Device
None	No login required.		X
Local	Uses local user/password for local authentication on the OnBoard.	X	X
Kerberos	Uses Kerberos network authentication protocol.	X	X
Kerberos Down/Local	Uses local authentication if Kerberos server is down.	X	X
Kerberos/Local	Uses local authentication if Kerberos authentication fails.	X	X
Local/Kerberos	Uses Kerberos authentication if local authentication fails	X	X
LDAP	Uses LDAP (Lightweight directory access protocol).	X	X
LDAP Down/Local	Uses local authentication if LDAP server is down.	X	X
LDAP/Local	Uses local authentication if LDAP authentication fails.	X	X
Local/LDAP	Uses LDAP authentication if local authentication fails	X	X

Table 1-2: Supported Authentication Types (Sheet 2 of 3)

Type	Description	OnBoard	Device
NIS/Local	Uses local authentication if NIS authentication fails. **Note:** If you select NIS authentication for the OnBoard or for any device, NIS must be used as the only authentication method for the OnBoard and all devices.	X	X
Local/NIS	Uses NIS authentication if local authentication fails.	X	X
RADIUS	Uses RADIUS authentication.	X	X
RADIUS Down/Local	Uses local authentication if RADIUS server is down.	X	X
RADIUS/Local	Uses local authentication if RADIUS authentication fails.	X	X
Local/RADIUS	Uses RADIUS authentication if local authentication fails.	X	X
SMB	Uses SMB authentication for Microsoft Windows NT/2000/2003 Domain.	X	X
SMB Down/Local	Uses local authentication if the SMB server is down.	X	X
SMB/Local	Uses local authentication if SMB authentication fails.	X	X
Local/SMB	Uses SMB authentication if local authentication fails.	X	X
TACACS+	Uses Terminal Access Controller Access Control System (TACACS+) authentication.	X	X
TACACS+ Down/Local	Uses local authentication if TACACS+ server is down.	X	X

Table 1-2: Supported Authentication Types (Sheet 3 of 3)

Type	Description	OnBoard	Device
TACACS+/Local	Uses local authentication if TACACS+ authentication fails.	X	X
Local/TACACS+	Uses TACACS+ authentication if local authentication fails.	X	X

Note: If a remote authentication method (like RADIUS) is specified without a local fallback option (like RADIUS Down/Local), when an administrative user logs in through the Web Manager or through the OnBoard console, then authentication always falls back to local authentication if the authentication server is not available. For any other types of logins, if an authentication method is specified without a local fallback option, and if the specified authentication server is not available, then authentication fails and the user cannot log in.

If configuring any authentication method other than Local, the administrator user must make sure an authentication server is set up for that method. The following list gives the prerequisites for configuring authentication servers.

- The OnBoard must be on the same subnet as an authentication server set up for every authentication method specified.
- Each authentication server must be configured and operational.
- The administrator configuring the OnBoard needs to work with the administrator of each authentication server to get user accounts set up and to obtain information needed for configuring access to the authentication server on the OnBoard.

For example, if LDAP authentication is to be used for logins to the OnBoard and if Kerberos authentication is to be used for logins to devices, then the OnBoard needs to have network access to both an LDAP and a Kerberos authentication server, and the administrator needs to perform configuration on the OnBoard for each type of authentication server.

An administrative user can use the Web Manager, and any administrator can use the `cycli` utility for configuring an authentication method for the OnBoard and for connected devices and for configuring authentication

servers. The tasks for configuring authentication are summarized in the following list with links to more information and to procedures using the Web Manager

Table 1-3: Tasks for Configuring Authentication

Task	Where Documented
Decide which authentication methods are going to be used for logins to the OnBoard and for logins to connected devices.	Table 1-2, "Supported Authentication Types," on page 5
Make sure an authentication server for each method is available to the OnBoard and work with the server(s)' administrators to obtain the information needed to configure the servers on the OnBoard and to make sure the required accounts are set up on the servers.	N/A
On the OnBoard, configure an authentication server for each authentication method.	"Configuring Authentication Servers" on page 179
Specify the OnBoard login authentication method or accept the default Local authentication method.	"Configuring an Authentication Method for the OnBoard" on page 192
Optional: create a custom security profile that defines a default authentication method to be assigned to all subsequently-created devices. (The specified authentication method can be overridden during configuration of new devices.)	"Selecting or Configuring a Security Profile" on page 224
While creating new devices assign the desired authentication method to each device.	"Configuring Devices" on page 163
Give users the login and password information they need for being authenticated on the devices.	

For examples of using `cycli` scripts to configure device authentication, see `/libexec/example_scripts`.

Understanding User and Group Configuration Options

On the OnBoard, two user accounts types are needed to give a user access to the OnBoard and to authorize the user for access to device management functions on connected devices:

- A normal UNIX user account
- An onboard user account

Both types of user accounts are created transparently when an administrator adds a new user using the Web Manager. When an administrator adds a new user through the `cycli` utility, the administrator needs to take a separate step and add both regular and onboard users separately

When setting up a user account, the administrator can do the following.

- Authorize the user to access the OnBoard by creating a user account and assigning a password to the account

  The user can access the OnBoard by using the Web Manager or `ssh`.
- Authorize the user to connect to the OnBoard using PPP or PPTP by specifying either or both types of access (PPP PPTP) and specifying a username and password
- Authorize the user to perform management actions on one or more connected devices.

  (For an overview, see “Management Features Available to Authorized Users and Groups” in the *AlterPath OnBoard User’s Guide*.)
- Authorize the user to perform administrative actions on the OnBoard by assigning the user to the preconfigured admin group.
- Assign the user to an administratively-configured group.

Parameters for Configuring Users

The OnBoard administrator configures user accounts by assigning parameters that are described in the following table. Where more information is needed, the table provides links to where the parameters are described in more detail.

Table 1-4: User Configuration Settings

Settings	Notes
Username	Login name required for the user account.
Full name	Administratively-defined name to identify the user.
Password	Password used for accessing the OnBoard.
• Sensors • Event log • Device Console • Power • Service Processor Console • Native IP	Allow the user to perform the selected device management actions. See "Management Features Available to Authorized Users and Groups" in the *AlterPath OnBoard User's Guide*.)
PPP/PPTP access • None • PPP (dialup only) • PPTP (VPN only) • PPP (dialup) and PPTP (VPN)	Allow the user to use PPP or PPTP or both for contacting the OnBoard. Requires a password, which may be different from the one required to access the OnBoard.

Configuring Groups

When configuring a group, the administrator can do the following:

- Assign users to the group
- Authorize the group to perform management actions on one or more connected devices.

In addition, administrators can do the following:

- Authorize users to manage outlets on optionally-connected AlterPath PM IPDUs
- Modify the menu displayed for all users at console login

Tasks for Configuring Users and Groups

The following table lists the most-common tasks related to user and group configuration with links to where the tasks are documented

Table 1-5: Tasks for Configuring Users and Groups.

To Create and Authorize a User for Device Management—Wizard	Page 107
To Create and Authorize a User for Device Management	Page 174
To Modify a User's Account	Page 175
To Create and Authorize a Group for Device Management	Page 177
To Configure a User to Manage Power Outlets on a Connected IPDU	Page 137
To Modify the Menu Displayed for Users at Console Login	Page 51

Planning Access to Connected Devices

Planning should include the following steps:

- Create a list of servers and other devices to connect to the OnBoard.
- If devices are going to be plugged into outlets on connected IPDUs, make a note of the outlets where the devices will be plugged (you need to supply the outlet numbers when configuring IPDU power management).
- Create a list of user accounts that specifies which type of access each user needs to which connected devices and to which IPDU outlets.
- Obtain usernames and passwords for connected devices or authentication servers to give to the users of connected devices.
- Provide the names of the servers and devices to authorized users for accessing device management actions using the `ssh` command.

Understanding Security Profiles

An important part of configuring the OnBoard is selecting a security profile that helps enforce the security policies of the organization where the OnBoard is being used.

Each OnBoard has a security profile defined during initial configuration. The type of security profile selected by the OnBoard administrator controls the following:

- Which services are turned on
- Whether a default authentication is specified for all subsequently-configured devices
- Whether authorizations are checked (bypassing authorizations is not available in any of the default security profiles, but it can be selected in a custom security profile)

The administrative user defines the security profile during initial configuration. The security profile can be changed later. Services can also be turned on and off independently from the security profile. For more details, see “Understanding Services on the OnBoard” on page 17.

The following tables describes the services that are enabled and disabled in the three types of preconfigured security profiles.

Table 1-6 describes the “Moderate” security profile.

Table 1-6: Moderate Security Profile Services/ Features

Enabled Services/Features	Disabled Services/Features
HTTP	RPC
HTTPS	SNMP v1
ICMP	SNMP v2c
IPSec	SNMP v3
PPTP	Telnet to OnBoard
SSH v1	
SSH v2	

Table 1-6: Moderate Security Profile Services/ Features (Continued)

Enabled Services/Features	Disabled Services/Features
Default authentication type to access devices set to Local	

Table 1-6 describes the “Secured” security profile

Table 1-7: Secured Security Profile Services/Features

Enabled Services/Features	Disabled Services/Features
HTTPS	HTTP
SSH v2	ICMP
Default authentication type to access devices set to Local	IPSEC
	PPTP
	RPC
	SNMP v1
	SNMP v2c
	SNMP v3
	SSH v1
	Telnet to OnBoard

Table 1-8 describes the “Open” security profile

Table 1-8: Open Security Profile Services/Features

Enabled Services	Disabled Services/Features
HTTP	None
HTTPS	
ICMP	

Table 1-8: Open Security Profile Services/Features (Continued)

Enabled Services	Disabled Services/Features
IPSec	
PPTP	
RPC	
SNMP v1	
SNMP v2	
SNMP v3	
SSH v1	
SSH v2	
Telnet to OnBoard	
Default authentication type to access devices set to Local	

Table 1-9 describes the services and other functionality that the administrator can select in the “Custom” security profile.

Table 1-9: Services and Other Functions in the “Custom” Security Profile (Sheet 1 of 3)

Option
FTP
ICMP
IPSec
PPTP
RPC
SNMP (Enables all versions of SNMP)

Table 1-9: Services and Other Functions in the “Custom” Security Profile (Sheet 2 of 3)

Option
SSH Options • Allow root login using SSH • SSH v1, SSH v2 (allow or disallow) • SSH Port (Assign an alternate port to SSH)
HTTP & HTTPS Options • Redirect HTTP to HTTPS • HTTP (allow or disallow) • HTTP port number (Assign an alternate port to HTTP) • HTTPS (allow or disallow) • HTTPS port number (Assign an alternate port to HTTPS)
Override authorization—enable access based on authentication only

Table 1-9: Services and Other Functions in the “Custom” Security Profile (Sheet 3 of 3)

Option
Default authentication type to access devices (applies to devices configured subsequently): • None • Local or NIS • Kerberos • Kerberos Down/Local • Kerberos/Local • Local/Kerberos • LDAP • LDAP Down / Local • LDAP/Local • Local/LDAP • Radius • Radius Down / Local • Radius/Local • Local/Radius • SMB • SMB Down / Local • SMB/Local • Local/SMB • TACACS+ • TACACS+ Down / Local • TACACS+/Local • Local/TACACS+

Understanding Services on the OnBoard

A network service is available on the OnBoard if one of the two following conditions are true:

- The security profile enables the service.
- The administrator has enabled the service through the Web Manager, or by using `cycli` or regular UNIX commands.

Administrators can turn services on and off by using the Web Manager Config → Services page or by using either the `cycli` utility or regular Linux commands.

Note: In the Web Manager, the security profile screen and the services screen detect when a service is enabled using either the Web Manager or `cycli` utility. If the administrative user unchecks a service in the Config → Services page, the custom security profile screen then shows the service as disabled, and vice versa. Similarly, if a service is enabled using either the Web Manager or the `cycli` utility, the `cycli` utility detects it. However, if the root user turns services on and off on the command line using Linux `start` and `stop` commands, the change in state for the service is not detected either by the Web Manager or the `cycli` utility.

If any of the services listed in the following table are enabled, the administrator must perform additional configuration in order for the services to work. The following table lists the services and where to configure them using the Web Manager.

Table 1-10: Services That Require Additional Configuration

Service	Where Documented
DHCP	“DHCP on the OnBoard” on page 25.
HTTPS	“HTTPS on the OnBoard” on page 23 and “To Replace the Self-Signed Certificate With an SSL Certificate From a Certificate Authority” on page 23.
IPSec	“VPN on the OnBoard” on page 32 “IPSec VPN Connections” on page 35

Table 1-10: Services That Require Additional Configuration (Continued)

Service	Where Documented
PPTP	"VPN on the OnBoard" on page 32 "Configuring Users and Groups" on page 169 "PPTP VPN Connections" on page 38
NTP	"Configuring System Date and Time" on page 150
SNMP	"SNMP on the OnBoard" on page 30.
Syslog	"Understanding Firewall/Packet Filtering on the OnBoard" on page 63
Telnet	"Telnet on the OnBoard" on page 19.

If enabled, the services in the following list are available to users without further configuration:

- FTPD
- HTTP
- ICMP
- INETD
- PMD
- RPC
- SSH

Passing OnBoard-specific service processor management commands as parameters to `ssh` on the command line is always enabled as long as the following are both true:

- The service processor supports the command
- The user is authorized to use that command for that service processor

(For details about the service processor management commands, see the *AlterPath OnBoard User's Guide*.)

Telnet on the OnBoard

By default, Telnet is configured as follows:

- Users cannot use Telnet to connect to the OnBoard or through the OnBoard to connected devices.
- The OnBoard uses Telnet to connect to devices on behalf of authorized users.

The following table shows the tasks for changing the default `telnet` configuration with links to where the tasks are documented.

Table 1-11: Tasks for Changing the Default telnet Configuration

Change to Default Telnet Configuration	Where Documented
Enable Telnet for users to use when connecting to the OnBoard or when connecting through the OnBoard to devices	"Configuring Telnet for Users" on page 19
Replace Telnet with SSH for the system to use when creating connections to devices on behalf of the authorized user from the OnBoard	"Configuring SSH or Bidilink Instead of Telnet for OnBoard to Device Connections" on page 20

Configuring Telnet for Users

The OnBoard uses Telnet when connecting to service processors except when connecting to IPMI service processors, when it uses `ipmitool` commands. Telnet is used in all other cases because some service processors do not support `SSH`.

The telnet service is not supported by any of the default security profiles and by default, `telnetd` is turned off. The OnBoard-specific service processor management commands cannot be passed as parameters to `telnet` on the command line. Telnet can be enabled by an administrative user on the Web Manager Config → Services page or by the root user, who can use normal Linux commands to start `telnetd` on the command line.

Caution! Because Telnet is not secure and not encrypted, its use by users for directly connecting to devices or to the OnBoard is strongly discouraged.

See "Configuring the OnBoard's Services" on page 229.

Configuring SSH or Bidilink Instead of Telnet for OnBoard to Device Connections

Telnet is not encrypted, so security can only be guaranteed if the service processors are on a private network. If the service processors must be on the public network for a pressing reason, then `telnet` should be replaced with SSH or `bidilink`. Instructions on replacing `telnet` as the connection method with SSH or `bidilink` are given in the `/usr/share/docs/OnBoard/Application_Notes/Service_Processor_Related/Alternate_Access` directory. See also the procedure below: "To Substitute SSH or bidilink for Telnet for Device Connections."

The root user can configure `ssh` to be used instead of Telnet on service processors that support `SSH`.

An OnBoard administrator who knows the root password and can connect to the console can follow the instructions in the `/etc/libexec/onboard/ssh_login.exp` file to enable ssh access.

▼ To Substitute SSH or bidilink for Telnet for Device Connections

1. Log into the OnBoard as root.
2. Change to the `/libexec/onboard` directory.

```
[root@OnBoard onboard] cd /libexec/onboard
```

3. To begin configuring `bidilink` as the device connection method, do the following steps.
   a. Copy `bidi_login.exp` to a new file, as shown in the following screen example.

```
[root@OnBoard onboard]# cp bidi_login.exp soe_login.exp
```

   b. Open the new file for editing and edit the appropriate options.

      For example, to use TCP without `telnet` commands being intercepted, you would need to uncomment and modify the line that

defines the bidilink PORT. The following screen example shows the line to change.

```
# spawn bidilink tcp-client::PORT
```

This example shows the comment (#) sign removed and changes `PORT` to `3301`.

```
spawn bidilink tcp-client::3301
```

c. When you are done editing the appropriate options, save and quit the file.

4. Copy the appropriate Expect script for the desired device type to a custom script name.

For example, if you want the OnBoard to use `ssh` or `bidilink` to communicate with iLO-type devices, copy the contents of `talk_ilo.exp` into the `talk_custom1.exp` file.

```
[root@OnBoard onboard]# cp talk_ilo.exp talk_custom1.exp
```

5. Open the custom expect script for editing, and find the line that sources the `common.exp` file.

```
source [file join [file dirname [info script]] "common.exp"]
```

6. To continue substituting `bidilink`, add a line to source the new file created in Step 3.

```
source [file join [file dirname [info script]] "common.exp"]
source [file join [file dirname [info script]]
"soe_login.exp"]
```

7. To begin substituting `ssh`, add a line to source the `ssh.login.exp` file

```
source [file join [file dirname [info script]] "common.exp"]
source [file join [file dirname [info script]]
"ssh_login.exp"]
```

8. Save and quit the file.
9. Assign the new custom type to the appropriate service processors.

   For example, if you have created a `talk_custom1.exp` for iLO service processors, configure the iLO service processors as custom1 type.

   If you are substituting `bidilink`, you are done.
10. If you are substituting `ssh`, set up host keys for every service processor configured to use `ssh` by doing the following steps.
    a. Use `ssh` to connect to the service processor as an administrator.

```
[root@OnBoard onboard]# ssh -t
administrator_name@OnBoard_DNS_name_or_IP_addr
```

A dialog similar to the following appears.

```
The authenticity of host 'SP (127.0.0.1)' can't be
established.
RSA key fingerprint is
5e:35:3d:0b:e8:3d:07:13:45:45:ad:6a:6f:2c:4c:aa.
Are you sure you want to continue connecting (yes/no)?
```

    b. If the fingerprint matches that of the Service Processor, answer yes.
    c. Enter the password when prompted.

HTTPS on the OnBoard

For HTTPS (secure HTTP based on SSL) to work, an SSL certificate must be present on the OnBoard. To reduce the risks posed by weaknesses inherent in self-signed certificates, OnBoard administrators are strongly advised to replace the automatically-generated self-signed certificate with an SSL certificate from an official certificate authority (CA). See `http://pki-page.org` for a list of certification authorities, if needed. See also the following procedure for how to generate a certificate signing request, and for how to install the public key and the certificate in the Apache web server on the OnBoard after you obtain the certificate from the CA.

▼ *To Replace the Self-Signed Certificate With an SSL Certificate From a Certificate Authority*

1. Log into the OnBoard console as root.
2. Use `openssl` with the `req` parameter to create a private key and a public CSR (certificate signing request).

   Use the command line shown in the following screen example.

Note: The command line in the screen example is broken into two lines because of space limitations. You can either enter the whole command on one line or include a backslash (\) as shown to tell the shell that the command continues on the following line.

```
[root@OnBoard /]# openssl req -new -nodes -keyout private.key -out \
public.csr
```

The utility prompts for information. The required information is shown in the following table. Any other requested information is not required.

Table 1-12: Required Information When Creating a SSL Certificate Request

Prompt	What You Enter
Country Name (2 letter code) [AU]:	The country code consisting of two letters.

Table 1-12: Required Information When Creating a SSL Certificate Request (Continued)

Prompt	What You Enter
State or Province Name (full name) [Some-State]:	The full name (not the postal abbreviation) of the state.
Locality Name (e.g., city) []:	The name of your city.
Organization Name (e.g., company) [Internet Widgits Ltd]:	The organization for which you want to obtain the certificate
Organizational Unit Name (e.g., section) []:	The department or section
Common Name (e.g., your name or your server's hostname) []:	The name of the machine where the certificate must be installed
Email Address []:	Your email address or the administrator's email address

The generated request automatically includes the public key.

3. Submit the CSR request to the certificate authority (CA).

   After receiving the certificate from the CA, do the remaining steps.

4. Copy the private key into `/etc/httpd/conf/ssl.key/server.key`.

```
[root@OnBoard /] cat private.key > /etc/httpd/conf/ssl.key/server.key
```

5. Copy the certificate into `/etc/httpd/conf/ssl.crt/server.crt`.

   The following screen example uses `cert.crt` as the name of the certificate file from the CA, Substitute the correct name for your file.

```
[root@OnBoard /] cat cert.cert > /etc/httpd/conf/ssl.crt/server.crt
```

Note: By default, the `/etc/httpd/conf/ssl.key/server.key` and `/etc/httpd/conf/ssl.crt/server.crt` files are listed in `/etc/config_files` so they can be automatically saved in the flash memory whenever the `saveconf` command is run or the administrative user saves the configuration files using the "Save" button on the Mgmt → Backup/restore screen.

6. Run the `saveconf` command to save the configuration in flash.

```
[root@OnBoard /] saveconf
```

7. Restart the web server to put the certificate into effect.

```
[root@OnBoard /] daemon.sh restart APACHE
```

DHCP on the OnBoard

Both a DHCP client and a DHCP server are available on the OnBoard.

DHCP Client

The OnBoard's DHCP client is active, with DHCP enabled by default for the primary Ethernet port. With the default configuration, if the OnBoard cannot find a DHCP server on the same subnet, it falls back to using the default IP address. For more about using DHCP and the default IP address, see the *AlterPath OnBoard Installation Guide*.

DHCP Server

A DHCP server (`dhcpd`) is present but disabled on the OnBoard by default. The OnBoard administrator may want to enable the DHCP server to provide fixed IP addresses for connected devices that are running DHCP client software. The fixed IP addresses use the following DHCP features:

- Persistent leases, which allow the device on the private side of the OnBoard to keep the same IP address even after the OnBoard or the device is powered down and up again.
- Persistent storage of lease information, with the `leases` file and the `dhcpd` configuration files stored in the flash memory and available to be optionally updated from time to time when `dhcpd` is enabled.
- Preconfigured leases: using the MAC address of the device, the OnBoard administrator can assign an IP address to a client before the OnBoard sees the device on the network.

Note: IP addresses assigned to connected devices must remain constant over time because each device is assigned an IP address as part of its configuration on the OnBoard. For that reason, the OnBoard DHCP server should not be used to provide dynamic IP addresses to devices.

The ability of DHCP to supply fixed addresses can be used to implement the addressing scheme for connected devices, which is described in the following sections of this manual:

- "Preparing an Addressing Scheme" on page 55
- "Understanding Address Configuration for Connected Devices" on page 336).

The OnBoard administrator can enable the DHCP server and assign IP addresses to devices by logging into the OnBoard command line as root and manually editing the `/etc/dhcpd.conf` file and performing other steps described under "Configuring the DHCP Server" on page 26.

Considerations When Deciding Whether to Use DHCP to Configure Device Addresses

Before deciding whether to use the DHCP server to configure addresses for connected devices, the OnBoard administrator should understand the available options for assigning IP addresses to connected devices, which are described in "Understanding Address Configuration for Connected Devices" on page 336.

Configuring the DHCP Server

To enable DHCP to configure IP address for connected devices, the administrator must perform DHCP configuration manually. The root user logs into the OnBoard command line and does the following steps.

- Enables the `dhcpd` by editing `/etc/dhcpd.sh`.
- Makes the appropriate configuration changes and specifies fixed addresses for all devices in the `/etc/dhcpd.conf` file.
- Saves the configuration file changes in the firmware using the `saveconf` command.
- Reboots or restarts the `dhcpd` service manually.

▼ *To Configure DHCP for Managing IP Addresses of Connected Devices*

1. Log into the OnBoard console as root.
2. Open the `/etc/dhcpd.conf` file for editing.
3. Copy and paste the `## SAMPLE CONFIGURATION ####` section.
4. Remove the comment (#) signs at the beginning of the lines.

```
# ######## SAMPLE CONFIGURATION ###############
subnet 192.168.0.0 netmask 255.255.255.0 {
      range 192.168.0.110 192.168.0.119;
      default-lease-time 86400;
      max-lease-time 172800;
      option broadcast-address 192.168.0.255;
      option routers 192.168.0.10;
      option subnet-mask 255.255.255.0;
      option domain-name-servers 192.168.0.11;
      option domain-name “cyclades.com.au”;
      host MySP {
            hardware ethernet 00:e0:4c:ec:12:26;
            fixed-address 192.168.0.211;
     }
}
# ##############################################
```

5. Configure a hostname and fixed address for each device by performing the following steps.
   a. Find the line that begins “host MySP,” and replace “MySP” with a hostname/alias for the device, for example, “host sp1.”

b. Specify the MAC address of the device on the line that begins "hardware ethernet," for example, "hardware ethernet 00:60:2e:bb:aa:aa."

c. Specify the desired IP address for the device on the line that begins "fixed-address," for example, "fixed-address 192.168.0.21."

For example, see the following edited host entry.

```
    host sp1 {
        hardware ethernet 00:60:2e:bb:aa:aa;
        fixed-address 192.168.0.21;
    }
# ##############################################
```

d. Copy and paste the three lines that define the IP address for a device as many times as needed and then make the edits to specify the desired IP address for each device.

6. Make other changes as appropriate for your environment, removing the comment (#) signs at the beginning of all edited lines.

7. Save and quit the file.

8. Open the `/etc/dhcpd.sh` file for editing.

```
# This file defines the dhcpd service configuration


ENABLE=NO                    # Must be "NO" or "YES" (uppercase)
DNAME=dhcpd                    # daemon name
DPATH=/usr/sbin                # daemon path
ShellInit=                     # Performs any required
initialization
ConfigFiles=/etc/dhcpd.conf             # configuration files
DTYPE=sig                      # must be "sig" or "cmd"
DSIG=kill          # signal to stop/restart the daemon
(lowercase)
                  # if it's hup term will be used to stop the
daemon
# daemon command line parameters
DPARM="-q priv0"
DSTOP=
```

9. Change the definition `ENABLE=NO` to `ENABLE=YES`.

```
ENABLE=YES                     # Must be "NO" or "YES"(uppercase)
```

10. Save and quit the file.

11. Save the configuration file changes by running the `saveconf` command.

```
[root@OnBoard /# saveconf
```

12. Start `dhcpd` by either restarting the OnBoard or restarting `dhcpd`.

The following screen example shows the syntax for restarting `dhcpd`.

```
[root@OnBoard etc]# daemon.sh restart DHCPD
```

SNMP on the OnBoard

The OnBoard administrator can activate Simple Network Management Protocol (SNMP) agent software that resides on the OnBoard so that the SNMP agent sends notifications about significant events or traps to administrators or to an SNMP management application, such as HP Openview, Novell NMS, IBM NetView, or Sun Net Manager. SNMP clients can also access SNMP data from the OnBoard or from connected service processors.

The OnBoard SNMP agent supports SNMP v1, v2c, and v3. The use of v3 is strongly encouraged because it provides authentication and encryption of data that is lacking in v1 and v2c.

The OnBoard provides proxied access to SNMP data from service processors.

The administrator can configure the following:

- General information provided by the OnBoard, including location and contact fields
- Who has access to SNMP information
- How traps are handled locally
- Trap forwarding

OnBoard traps occur on the following types of events:

- Interface up/down
- PCMCIA card insertion/removal
- Power supply events.

SNMP information provided by the OnBoard and by service processors is accessible two ways:

- The recommended method of access for clients which support only SNMP version 1 or 2c is through a VPN tunnel to the OnBoard. The OnBoard provides the authentication and encryption lacking in those protocol versions.

Caution! The `snmpd` running on OnBoard allows access to proxied data using the v1 and 2c protocols without the creation of a VPN tunnel, but the lack of security inherent in these protocols means this option should be used with caution if it is used at all.

- The method of access for clients which support version 3 is via a local Net-SNMP snmp daemon. The proxying of traps is not supported, but forwarding of traps is supported, with filtering by source address.

If SNMP is used as recommended (by allowing access by hosts running SNMP clients at version 1 and 2c only through a tunnel), no public client is allowed unauthenticated access to either managed clients or to the OnBoard itself. For compatibility with other clients, unencrypted transfer of data is possible with SNMP v3 connections, but unencrypted data transfer is strongly discouraged.

Caution! Because of the risks in unencrypted data transfer, connections should be encrypted whenever possible.

Views describe the sections of an OID tree that are included and excluded from access. When a view is being defined, more than one line can be used to build a view. For example, one line may allow access to a subtree, and another may remove access to a portion of that subtree.

The following table shows the tasks related to administering SNMP on the OnBoard and provides links to where they are documented.

Table 1-13: Tasks for Configuring SNMP

Task	Where Documented
Configure SNMP on the OnBoard	"Configuring SNMP" on page 209 "To Configure SNMP Trap Notifications" on page 196
Activate the SNMP service	"Configuring the OnBoard's Services" on page 229

VPN on the OnBoard

As described in the *AlterPath OnBoard User's Guide*, for security reasons an authorized user must establish a trusted connection with the OnBoard before accessing certain management features that are available on connected service processors. (In the user's guide, see "Native IP" for details about the service processor management actions that require a trusted connection and see "Making VPN Connections" for what the user needs to know and do.)

Users can access devices only if an OnBoard administrator has authorized them to do so. For example, user sherlock may be authorized to access the OnBoard and two connected devices on the private network, deviceA and deviceB, while user jedgar may be authorized to access deviceA, deviceC, and deviceD.

Caution! Once a user has been authenticated and the user's authorizations to access a device have been checked, the user with a VPN connection has unlimited access to the device. Since the OnBoard cannot control whether a connected device allows unrestricted access to the rest of the network, the administrators of connected devices must take care to configure the connected devices in such a way as to control the access of individual users on individual devices to maintain the security of the network.

VPN connections establish encrypted communications between the OnBoard and the remote host. The encryption creates a security tunnel for communications through an intermediate network which is untrustworthy. The remote host and the OnBoard take care of encryption and decryption on their end.

The remote host must have support for one of the following types of VPN:

- IPSec
- PPTP

VPN Client System Requirements and Limitations

The following table describes the VPN client system requirements and limitations tor different platforms and VPN services.

Table 1-14: VPN Client System Requirements and Limitations

Platform	PPTP	IPSec
Windows	• Windows XP • Windows 2000 • Windows NT • Windows ME • Windows 98 • Windows 95 with DUN1.3 update Supported authentication method: MS-CHAPv2 **Note:**Only local or RADIUS authentication types can be used because the MS-CHAPv2 protocol does not work with other authentication types, such as LDAP, Kerberos, or TACACS+.	• Windows XP • Windows 2000 Supported authentication types: • X.509 certificates (which require the administrator to manually create the certificate files in `/etc`) • RSA public key • Preshared key (PSK) requires a static IP
Linux	PPTP client (pptp-linux)	OpenSWAN
MacOS X	Internet Connect application	MacOS X 10.2 or later

Configuring VPN

This section describes what the administrator must do to enable VPN on the OnBoard side to support the users' VPN connections.

The OnBoard administrator must do the tasks shown in the following table.

Table 1-15: Tasks for Configuring VPN Connections

Task	Where Described
Make sure that the appropriate service for the desired type of VPN connection is enabled (either PPTP or IPSec).	"Understanding Services on the OnBoard" on page 17
Configure a VPN connection profile on the OnBoard for the type of VPN connections that are being used.	"Configuring VPN Connections" on page 246 Also see examples under: "Understanding Address Configuration for Connected Devices" on page 336

The user must do the tasks in the following list to configure a VPN, with more details described in the following sections:

- Obtain from the OnBoard administrator the values used in creating the VPN connection profile on the OnBoard end including the PPTP username and password if PPTP is being used.
- Configure a VPN connection profile on the user's remote computer.
- If a route is needed to enable the user's workstation and the OnBoard to exchange packets, specify it in the IPSec connection profile or create a route manually.
- Before attempting to access the "Native IP" feature on the OnBoard, the user must start the VPN connection from the user's computer.

The OnBoard listens for the connection attempt from the IP addresses specified in its connection profiles and grants the access.

IPSec VPN Connections

For a user to access native IP functionality on a connected service processor, the user needs to create a VPN connection to the OnBoard; launching an IPSec VPN connection requires the user to have IPSec running on the computer being used to manage OnBoard-connected devices.

The ESP and AH authentication protocols (also called “encapsulation methods”) are supported. RSA Public Keys and Shared Secret are also supported. Authentication information (username and password and connection keys or certificates) is needed.

If the RSA public key authentication method is chosen, the generated keys are different on each end. When shared secret is used, the secret is shared on both ends.

The values needed for configuring IPSec VPN connections can shown in the following table.

Table 1-16: IPSec VPN Configuration Information for Administrators and Users

Value Name	Description
Connection Name	Any descriptive name you choose.
Authentication protocol	• AH • ESP
Authentication method	• RSA public keys • Shared secret
Boot action	• Ignore • Add • Start • Add and route
Remote (“Right”)	
ID	*@workstation_name.*
IP address	IP address of the user’s workstation.

Table 1-16: IPSec VPN Configuration Information for Administrators and Users (Continued)

Value Name	Description
Next hop	Leave blank if the user's workstation and the OnBoard are able to exchange packets. If a route must be set up to enable communications, enter the IP address of a host or network, so the IPSec can use the IP address to set up the needed route. Requires the "Add and route" boot option to also be selected.
Subnet	Leave blank.
Preshared key	Required if shared secret is selected as the authentication method.
RSA key	Required if RSA public keys is selected as the authentication method. The generated key for the remote computer, which the OnBoard administrator must obtain from the user.
Local ("Left")	
ID	*@OnBoard_name.*
IP address	Public IP address of the OnBoard.
Next hop	Leave blank if the user's workstation and the OnBoard are able to exchange packets. If a route must be set up to enable communications, enter the IP address of a host or network, so the IPSec can use the IP address to set up the needed route. Requires the "And and route" boot option to also be selected.
Subnet	Network IP address and netmask for the private subnet where the devices reside that are going to be accessed through the OnBoard.
Preshared key	Required if shared secret is selected as the authentication method
RSA key	Required if RSA public keys is selected as the authentication method. The administrator generates an RSA key for the OnBoard

The OnBoard administrator must do the following tasks:

- Make sure that the IPSec service is enabled.
- Configure an IPSec VPN connection profile on the OnBoard.
- Give the user a copy of the parameters used to configure the IPSec connection profile on the OnBoard.

  The OnBoard administrator can send a copy of the relevant portions of the `ipsec.conf` file after the changes are saved and applied in the Web Manager for the user to insert into the `ipsec.conf` file on the user's workstation.

The authorized user must do the following tasks:

- Use the same values used by the OnBoard administrator to create an IPSec VPN connection profile on the user's workstation.

  If the OnBoard administrator sends the relevant portions of the `ipsec.conf` file from the OnBoard's IPSec configuration, use it to replace the same section in the workstation's `ipsec.conf` file.
- Ensure that routes are in place to allow IPSec communication with the OnBoard and also to allow packets to the device to be routed through that tunnel.
- Create the IPSec VPN connection.

Note: If a virtual network has not been configured, the user may need to create a separate tunnel to each private subnet they wish to access. If a virtual network has been configured, the user needs only to create a single tunnel to the virtual network.

- Use either a browser or `ssh` on the command line to access the OnBoard, using the OnBoard-side IP address assigned to the OnBoard; use the OnBoard-side IP address configured when the private subnet or virtual network to which the tunnel is connected was being configured.
- Through the OnBoard, enable native IP access to the device.

PPTP VPN Connections

For an authorized user to access native IP functionality on a connected service processor, the user needs to create a VPN connection to the OnBoard. An authorized user can create PPTP VPN connections from Linux, Windows, or Macintosh operating systems.

The tasks listed below must be performed by the OnBoard administrator before any user can make a PPTP VPN connection:

- Create a VPN connection profile on the OnBoard specifying a pool of addresses for the OnBoard and for the remote user's computer at the other end.

  When the user creates the PPTP VPN connection, PPTP creates a new virtual interface on the user's host and assigns an IP address from the OnBoard's IP address pool to the interface. The user must use this address when connecting to the OnBoard to enable native IP access to a device.
- Authorize the user for PPTP access and provide the user with the PPTP password, which may be different from the password that the user uses for accessing the OnBoard.
- Authorize the user for native IP access to a device or multiple devices.

The user must do the following tasks to enable PPTP on the user's workstation:

  Make sure the workstation can access the OnBoard by entering the OnBoard's public IP address in a browser to try to bring up the Web Manager.
- If a network or host route is needed, create a route to the private subnet where the device resides or to the real or virtual IP address of the device.
- Make sure a PPTP client is running on the user's workstation.
- Configure a PPTP VPN connection profile with the following information obtained from the OnBoard administrator:
  - PPTP server address = OnBoard public IP address (203.1.2.3)
  - Username = OnBoard user name
  - Password = PPTP password
- Make the PPTP VPN connection.

- Enter the `ifconfig` or `ipconfig` command on the command line of the user's workstation to discover the IP address assigned to the OnBoard's end of the PPTP link.
- Enter the OnBoard's PPTP-assigned address either in a browser or with `ssh` on the command line to access the OnBoard.
- Create a static route to inform the workstation that the devices to be contacted are at the other end of the point-to-point link at the OnBoard's PPTP-assigned address.
- If multiple private subnets have been configured without a virtual network (DNAT), then create a route for each subnet.
- Access the device and enable native IP access.

Caution! Remind users to always disable native IP before closing the PPTP VPN connection to prevent other users from potentially being able to obtain unauthorized and unauthenticated access to native IP features of the device.

Message Logging (With Syslog) on the OnBoard

The administrator can set up logging of messages about the following types of events:

- Events of interest from the OnBoard system
- Events of interest obtained by filtering data during device console connections with connected devices
- Overcurrent status from a connected AlterPath PM IPDU
- Sensor alarms generated by sensors on connected devices

Messages can be sent to central logging servers, called syslog servers. Messages can also be sent to the console or to the root user or both.

Message Filtering Levels

Messages can be filtered according to their severity, based on any or all of the levels that the administrator can select from the following list.

- 0 - EMERG
- 1 - ALERT
- 2 - CRIT

- 3 - ERROR
- 4 - WARNING
- 5 - NOTICE
- 6 - INFO
- 7 - DEBUG

Syslog Servers

Syslog servers run on operating systems that support system logging services, usually UNIX-based servers with the `syslogd` configured.

Before configuring syslogging, the OnBoard administrator must ensure that an already-configured syslog server with a public IP address is accessible from the OnBoard. The OnBoard administrator must know the IP address of the syslog server.

Tasks for Configuring Syslog Messages

The following table lists the tasks related to configuring syslog messages and destinations.

Table 1-17: Tasks for Configuring Syslog Messages

Task	Where Documented
Specify one or more syslog servers, optional additional destinations for syslog messages, and configure message filtering	"To Configure the Syslog Destination and Message Filtering" on page 221
Specify sensor alarms to be sent as syslog messages	"To Begin Configuring a Sensor Alarm" on page 202
Specify overcurrent alerts to be sent as syslog messages	"To Enable Overcurrent Protection for an AlterPath PM IPDU" on page 135

Understanding Ethernet Ports on the OnBoard

The OnBoard's two public Ethernet ports are used for connecting to the public (or management) network. The managed private side of the OnBoard (which is made up of 24 or 40 private Ethernet ports) is isolated from the public side to ensure security. Access to all connected servers is consolidated through the one publicly known IP address.

Private Ethernet Ports

The OnBoard is aware of only a single interface to the private network: priv0. for communicating with the connected devices. priv0 sends packets to and receives packets from the 24 or 40 private Ethernet ports.

Private Ethernet ports on the OnBoard are connected to the service processors' or other device's dedicated Ethernet ports.

Each private Ethernet port may be connected to multiple service processors, for example through a blade manager that has multiple service processors, and in those cases a single private Ethernet port may require multiple IP addresses.

All communication among private Ethernet ports are blocked unless priv0 is the sending or receiving port.

Public Ethernet Ports

On the public side of the OnBoard, the primary and secondary Ethernet ports are referred to as `eth0` and `eth1`. Optionally-added Ethernet PCMCIA cards are referred to as `eth2` and `eth3`, and if they are present, they are treated as public interfaces.

The secondary Ethernet port on the OnBoard can optionally be configured for failover, which is also referred to as bonding. Failover is important for high-availability environments where constant accessibility is required to support mission-critical applications. Failover automatically redirects traffic from the primary Ethernet port to the secondary Ethernet port if the primary interface fails. The primary Ethernet port continues to be monitored, and when it starts functioning again, traffic is then automatically redirected back through the primary Ethernet port again. All connection sessions continue without interruption.

With failover, both the primary and secondary Ethernet ports are assigned a single IP and single MAC [Ethernet] address.

After failover is enabled, the bonded Ethernet interfaces are referred to as "bond0."

For example, when failover is set, the `ifconfig` command lists `bond0` along with `eth0` and `eth1` as shown in the following screen example. Note that the "HWaddress" [MAC address] and "inet addr" [IP address] are identical for `bond0`, `eth0`, and `eth1`.

```
[root@ONB /]# ifconfig

bond0   Link encap:Ethernet  HWaddr 00:60:2E:00:4F:97
        inet addr:172.20.0.131  Bcast:172.20.255.255  Mask:255.255.0.0

eth0    Link encap:Ethernet HWaddr 00:60:2E:00:4F:97
        inet addr:172.20.0.131 Bcast:172.20.255.255  Mask:255.255.0.0

        ...
eth1    Link encap:Ethernet  HWaddr 00:60:2E:00:4F:97
        INET ADDR:172.20.0.131  BCAST:172.20.255.255  MASK:255.255.0.0
```

Tasks for Configuring Ethernet Ports

The following table lists the tasks the administrator must do to configure Ethernet ports on the OnBoard with links to sections that describe how to perform that tasks using the Web Manager.

Table 1-18: Tasks for Configuring Ethernet Ports

Task	Where Described
Configure Ethernet ports: • Primary only • Primary and secondary • Failover	• "Configuring Network Interfaces—Wizard" on page 91 • "To Configure OnBoard Network Interfaces—Wizard" on page 96 • "Configuring Network Interfaces" on page 233 • "Configuring Network Interfaces" on page 233

Understanding Modem Access Through the OnBoards

The OnBoard administrator can configure dial-in or callback access to the OnBoard through any of the two following types of modems:

- Optional external modem
- Optional PCMCIA modem card

The PCMCIA modem card can also be accessed from a terminal emulation program. Configuration is needed to enable dial-in and callback access to the OnBoard.

The following table lists the modem configuration tasks for the two types of modems, with links to where they are documented.

Table 1-19: Tasks for Configuring and Installing Modems

Modem Type	Where Documented
External modem	• "To Connect an External Modem to an AUX Port" in the *AlterPath OnBoard Installation Guide* • "Configuring the AUX Port for a Modem" on page 129
PCMCIA modem card	• "To Install a PCMCIA Card in the Front Card Slot" in the *AlterPath OnBoard Installation Guide* • "Configuring a Modem PCMCIA Card" on page 143

Note: Administrators can also configure modems through the `cycli` utility.

The following table shows the modem configuration options that apply whether the modem is being configured through the Web Manager or the `cycli` utility.

Table 1-20: Modem Configuration Field and Menu Definitions (Sheet 1 of 3)

Field or Menu Option	Options
Modem Access Type	Autodetect Login PPP
Baud Rate	300 to 460800
Flow Control	none hard soft both

Table 1-20: Modem Configuration Field and Menu Definitions (Sheet 2 of 3)

Field or Menu Option	Options

Modem Initialization	The modem chat string is used to configure the modem when it is turned on or when the communications software calls another modem. An example follows:
	`TIMEOUT 10`
	`"" \d\l\dATZ`
	`OK\r\n-ATZ-OK\r\n ""`
	`TIMEOUT 10`
	`"" ATM0`
	`OK\r\n ""`
	`TIMEOUT 3600`
	`RING ""`
	`STATUS Incoming %p:I.HANDSHAKE`
	`"" ATA`
	`TIMEOUT 60`
	`CONNECT@ ""`
	`STATUS Connected %p:I.HANDSHAKE`

Local IP Address	The local IP address used by PPP to set up the session between the local and the remote modem. By default, the IP address of the OnBoard is used. Use the default unless you have a specific reason to use another IP address.
Remote IP Address	The remote IP address used by PPP to set up the session between the local and the remote modem. By default, the IP address 10.0.0.1 is used. Use the default unless you have a specific reason to use another IP address.
Authentication Required	Require authentication or not.
MTU/MRU	The maximum transmission unit / maximum receive units for PPP type connections. Default MTU=1500 MRU=1500

Table 1-20: Modem Configuration Field and Menu Definitions (Sheet 3 of 3)

Field or Menu Option	Options
PPP Options	Some common options are: `auth -chap +pap login debug`
Callback	If callback is selected, a callback number must be entered.

Understanding Power Management Options on the OnBoard

Authorized users and OnBoard administrators can power off, power on, and reboot devices in two different ways. As described in the *AlterPath OnBoard User's Guide*, the OnBoard provides the following two types of power management options for administrators and authorized users:

- IPDU power management
- Service processor power management

IPDU Power Management

Authorized users can manage power for any type of device that is plugged into an AlterPath PM intelligent power distribution unit (IPDU), when the IPDU is connected to the OnBoard's AUX port and an administrator has configured the AUX port for power management.

Administrators can configure the OnBoard's AUX port and configure users to manage outlets on a connected IPDU using the following:

- Web Manager
- The `cycli` utility

Authorized users can manage outlets by using the Web Manager.

IPDUs can be daisy-chained. The number of outlets on all daisy-chained IPDUs cannot exceed 128.

Service Processor Power Management

Authorized users and administrators can manage power for a server whose service processor is connected to the OnBoard when the service processor provides power management capabilities.

OnBoard administrators and other authorized users most-commonly perform service processor power management through the Web Manager or through service processor management commands that can be passed as parameters to the `ssh` command.

Tasks for Configuring Power Management

The following table lists the tasks for configuring power management and where they are described.

Table 1-21: Tasks for Configuring Power Management

Task	Where Documented
Configure IPDU power management by doing the following:	
• Connect one or more AlterPath PM IPDUs to the AUX port • Configure the AUX port for IPDU power management • Configure users for IPDU power management	• "Connecting One or More IPDUs to the AUX Port" in the *AlterPath OnBoard Installation Guide* • "Configuring the AUX Port for Modem or Power Management" on page 127 • "Configuring Users to Manage Power Outlets on a Connected IPDU" on page 135
Configure service processor power management by doing the following:	
• Configure users for service processor power management	"Configuring Users" on page 170

Configuring the User's Console Login Menu

As described under "Using SSH with the OnBoard" in the *AlterPath OnBoard User's Guide*, regular users are configured with `/usr/bin/rmenush` as their default login shell. All users with `rmenush` as their login shell see the same menu whenever they log into the OnBoard's console.

The OnBoard administrator can configure the `rmenush` menu to display other options including links to additional submenus or commands by modifying the `/etc/menu.ini` file.

The default `/etc/menu.ini` file is shown in the following screen example.

```
# $Id: menu.ini,v 1.1 2005/06/23 21:37:07 scott Exp $
# Default menu for restricted shells

[main]
        Access_Servers = /bin/onbdshell
        Change_Password = /usr/bin/passwd
#         Submenu_1 = submenu1

[submenu1]
        Bash = /bin/bash
        Another_Submenu = submenu2

[submenu2]
        Example_with_compound_sleep = echo "Sleeping for 5
seconds";sleep 5
        Example_without_failure = cat /dev;/bin/true
        Example_with_failure = ps -ef;exit 1
        Unquoted_hash = echo #test;sleep 5
    Quoted_hash = echo "#test";sleep 5
```

Figure 1-1: Default `/etc/menu.ini` File

Caution! If changing the default menu, the administrator needs to ensure that any added programs do not introduce security vulnerabilities.

The administrator needs to know the following about the behavior of `rmenush` before configuring any changes to the menu:

- If the called program exits with a return code indicating an error, `rmenush` prompts the user to press any key to continue.
- Any error messages generated by the called program are left on the screen for the user to read. Examples show how the administrator can force this behavior on for successful programs and off for unsuccessful ones are provided in the configuration file.
- The OnBoard administrator assigns the `/usr/bin/rmenush` shell to users as appropriate, by editing the `/etc/passwd` file entries for the users.

When editing the `menu.ini` file, the administrator needs to know the following:

- Spaces are shown in menu items by the use of an underscore between words.
- The underscore cannot be displayed in the menu text.
- The right hand value of each name/command pair is assumed to be either a menu defined in the menu.ini file or a command.
- A maximum of sixteen menu items can display on the screen at a time. Any extra menu items can be reached by using the arrow keys to scroll down.

The OnBoard administrator can add options as shown in the following example.

New Menu Item Example

This example shows how the administrator could add the item shown in the Figure 1-2 to the user's login menu by adding the option shown in Table 1-22 to the `/etc/menu.ini` file.

Table 1-22: Example: Option Added to Menu for Regular Users

New Option	Function and Submenu	
`Onetime Password`	Displays the onetime password menu:	
	Menu Option	Function
	`opiepasswd`	Launches `/usr/bin/opiepasswd`
	`opipkey`	Executes `/usr/bin/opiekey`

The new option is added to the example `/etc/menu.ini` file in the following screen example.

```
# $Id: menu.ini,v 1.1 2005/06/23 21:37:07 scott Exp $
# Default menu for restricted shells

[main]
        Access_Servers = /bin/onbdshell
        Change_Password = /usr/bin/passwd
        Onetime_Password_Menu = opie
#        Submenu_1 = submenu1

[opie]
        opiepasswd = /usr/bin/opiepasswd
        opiepkey = /usr/bin/opiekey
```

Figure 1-2: Example: Onetime Password Option Added to `menu.ini`

▼ *To Modify the Menu Displayed for Users at Console Login*

Caution! If adding programs to the menu, take care the commands do not allow the user to break out of the programs they call.

1. Open a console session and log into the OnBoard as root.
2. Open the `/etc/menu.ini` file for editing.
3. Add new menus and menu items as desired.
4. Save and quit the file.

Understanding Routing on the OnBoard

The OnBoard administrator can configure routing for the following types of routes using either the Web Manager or the `cycli` utility.:

- default—See "Default Route Configuration
- host or network—See “Host or Network Route Configuration” on page 51

Default Route Configuration

Configuring the network interfaces sets up a *default route* for the interface.

- When DHCP is enabled for a network interface, the DHCP server assigns a default route to the interface.
- When DHCP is not enabled, if a gateway IP is specified by the OnBoard administrator for a network interface, the gateway IP is used to create a default route.

Host or Network Route Configuration

If a *host route* or network route is required, the route is configured as a static route that applies to the primary interface.

Tasks for Configuring Routes

The following table lists the tasks for configuring routing, and either lists the sections where the tasks are documented or provides the related `cycli` utility parameters.

Table 1-23: Tasks for Configuring Routes

Task	Where Described/Description
Assign a default route (Web Manager}	• "Configuring Network Interfaces" on page 233 • "To Configure OnBoard Network Interfaces" on page 237
Assign a default route (`cycli`)	On an already-active network interface: `cli> set network interface` *interface_name* \ `gateway` *gatewayIP*
Assign a host or network route {Web Manager}	• "Configuring Static Routes" on page 244 • "To Add a Static Route" on page 245
Assign a host or network route (`cycli`)	On an already-active network interface: • `set network st_routes` *hostIP* OR • `set network st_routes st_routes` *networkIP*/*NN*

Understanding OnBoard Notifications and Sensor Alarms

The OnBoard administrator can configure alarms of two different types using either the Web Manager or the `cycli` utility. The alarms may be triggered by the either of the following:

- System daemons (such as messages from the `cron` daemon, `crond`)
- Out of range sensor readings from sensors on service processors

When system events are the triggers, notifications can be sent to an OnBoard administrator by one of the following methods:

- SNMP trap
- Pager
- Email

The OnBoard administrator can configure periodic checks of sensor readings from service processors. Alarms can be set up to be triggered according to rules based on sensor values. When sensor readings are the triggers, alarms can be sent to OnBoard administrators by one of the following methods

- Syslog message
- SNMP trap
- Pager
- Email

When email is selected as a method for delivering notifications, an email address must be specified. See the following sections for how administrative users can configure notifications and alarms and email:

- “Configuring Notifications” on page 194
- “Configuring Sensor Alarms” on page 201
- “Configuring an Address for System Emails” on page 250

Understanding Device Configuration

When connecting devices to the OnBoard, observe the following recommendations, which are illustrated in Figure 1-3:

- Connect the main Ethernet port(s) on connected servers or devices to a *production* network, which must be accessible to all those who need to access the device.
- Connect the dedicated Ethernet port on each service processor or device to one of the OnBoard’s private Ethernet ports. The connections between the OnBoard and devices make up the *management network*.
- Connect the OnBoard’s primary Ethernet port (`eth0`) to a local management network and usually to the Internet, which extends the management network to remote users whose access to devices is controlled by the OnBoard.

Caution! If a device has a single Ethernet port, that port would need to be attached to the production network, and the OnBoard would be need to be configured to communicate with the device over the production network. With this type of configuration, the OnBoard would be unable to provide the same level of secure access to devices that it provides when it is configured as recommended.

Figure 1-3 illustrates connecting two servers that have service processors, with the service processors indicated by gray boxes. (The same recommendations apply to connecting devices that do not have service processors but that have dedicated Ethernet ports that provide access to the devices' consoles.) In Figure 1-3, note the following:

- The service processors' (SPs) dedicated Ethernet ports are connected to the OnBoard's private Ethernet ports.
- The servers' Ethernet ports are connected to the production network.
- The OnBoard's primary Ethernet port (eth0) is connected to a management LAN and to the Internet.

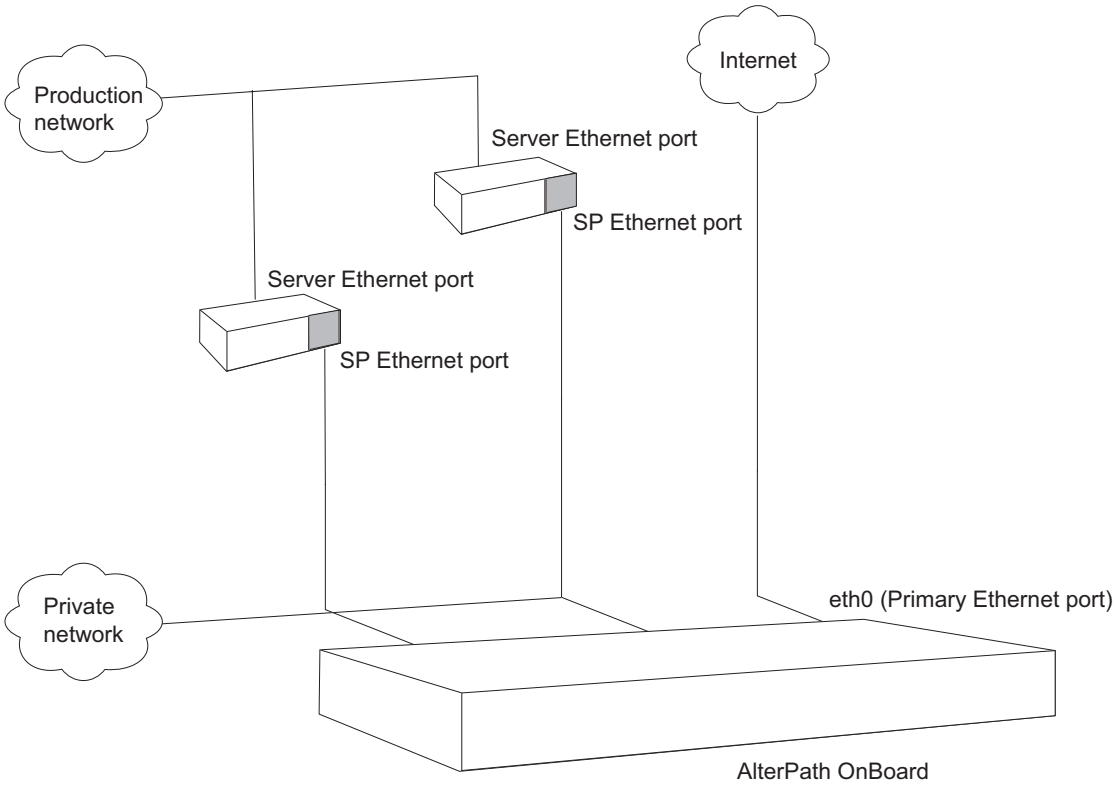


Figure 1-3: Recommended Device Configuration

Preparing an Addressing Scheme

Before configuring any connected devices, the OnBoard administrator must plan and implement an IP addressing scheme that reflects the needs of the organization.

As illustrated in Figure 1-3 the dedicated Ethernet ports on service processors and on other supported types of devices are connected to the private Ethernet ports on the OnBoard. Each connected device's dedicated Ethernet port needs an internal IP address assigned on the OnBoard and configured for the interface. By implementing an addressing scheme, the administrator creates a pool of internal addresses that can be assigned to the devices' dedicated Ethernet ports and configured for the device on the OnBoard side.

The following Figure 1-4 shows some example IP addresses assigned:

- A managed public IP address is assigned the OnBoard's eth0 Ethernet port: 203.1.2.3

  The OnBoard requires only one managed public IP address assigned to its primary Ethernet port. The OnBoard's secondary Ethernet port (`eth1`) can optionally be used as described under "Understanding Ethernet Ports on the OnBoard" on page 41.

- A private subnet IP address is assigned to each service processor's dedicated Ethernet port (192.168.49.60 and 192.168.49.61) from a *private subnet* network IP range of 192.168.49.0/24.

Note: The IP addresses assigned to the servers' primary Ethernet ports on the production network are not covered in this document; server's IP addresses can be whatever suits the needs of the servers' network administrators.

- A private IP address is assigned to the OnBoard from the same range as the devices' IP addresses: 192.168.49.254.

  While implementing the addressing scheme, the administrator assigns to the OnBoard itself one or more IP addresses in addition to the OnBoard's public IP address. The OnBoard's private IP address or addresses are used by the following:

  - By devices when talking to the private Ethernet ports of the OnBoard
  - By users who make PPTP or IPSec VPN connections to enable native IP access

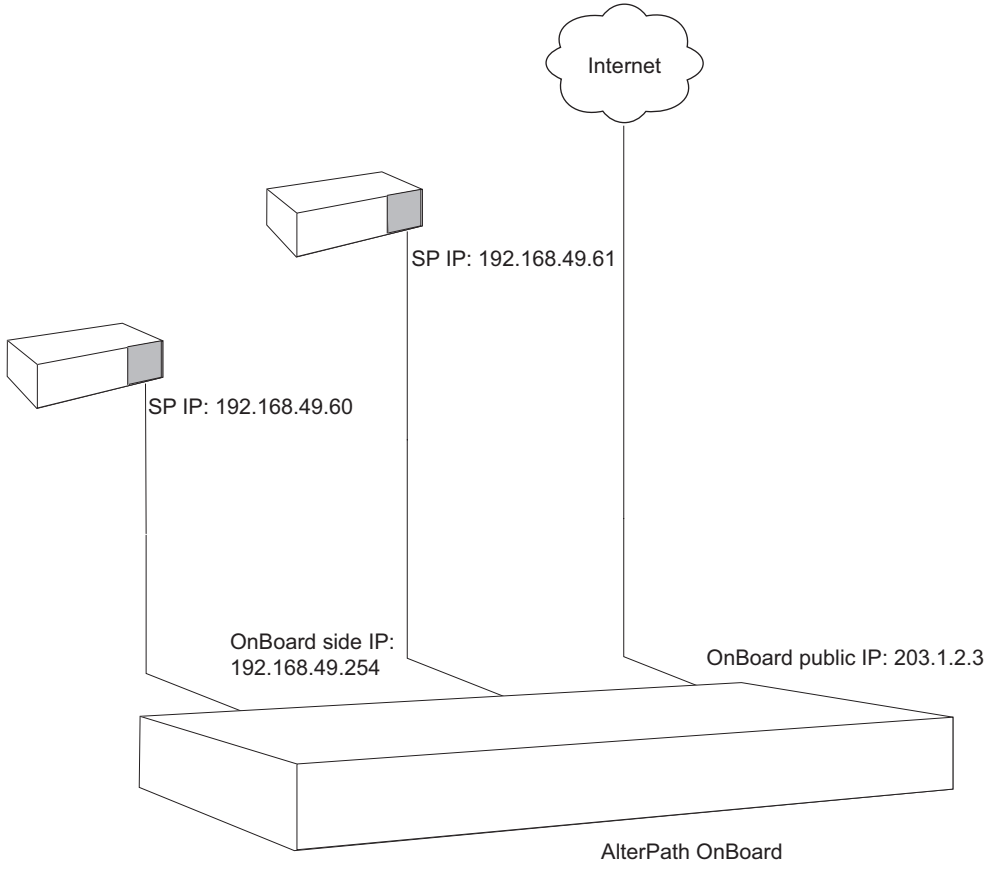


Figure 1-4: IP Addressing Example

See “Understanding Address Configuration for Connected Devices” on page 336 for the details needed for planning and implementing IP addresses. The referenced section describes the following topics that the administrator needs to understand:

- Why one or more private subnets must be created
- When virtual networks (using DNAT) must be created

Parameters for Configuring Devices

The OnBoard administrator configures connected devices by assigning parameters that are described in the following table. Where more information is needed, the table provides links to where the parameters are described in more detail.

Table 1-24: Device Configuration Parameters

Parameter	Description
Name	Also referred to as an *alias*. A meaningful string that helps identify the device and possibly its location, such as `rack1_dev1_ibm306_rsa` for an IBM 306 in the bottom row of rack 1. The assigned name can be used to access the device by entering the name with the `ssh` command on the command line. See the *AlterPath OnBoard User's Guide* for the syntax for using `ssh` with a device's name to perform device management functions on the server or other device.
Login name and password	Obtained from the server's or device's administrator. Can be different from the user name and password pair that the user enters used to access the OnBoard.
Type	The type of service-processor-management protocol or type of access. The following lists each of the defined service processor and device types. • iLO • RSA II • DRAC • IPMI 1.5 • device console • custom1 • custom2 • custom3 See "Device Type Differences" on page 312" for more information about assigning the correct device type.

Table 1-24: Device Configuration Parameters (Continued)

Parameter	Description
Command template (where required for the selected device type)	A template that contains text commands that manage communications between the user and the connected device and performs device management actions. See “Command Templates” on page 321 in Appendix A, “Advanced Device Configuration,” which provides additional background information and a procedure for choosing or creating a command template to work with a device.
Private subnet name/ Addr	Used by the OnBoard to communicate with devices on the private network. See “Understanding Private Subnets on the OnBoard” on page 61 and “Why Define Private Subnets?” on page 339 for more information about planning and implementing subnets and assigning them to devices. Private subnets can be configured in the Web Manager on the Wizard Subnets screen or on the Network Private Subnets screen as described in the following sections: • “Configuring Private Subnets and Virtual Addresses—Wizard” on page 98 • “Configuring Private Subnets and Virtual Networks” on page 251.
Device IP address	An IP address used by the OnBoard to communicate with the device. See “Preparing an Addressing Scheme” on page 55 “Understanding Address Configuration for Connected Devices” on page 336 and “Options for Assigning IP Addresses to Connected Devices” on page 368 for more information about assigning IP addresses.

Table 1-24: Device Configuration Parameters (Continued)

Parameter	Description
Virtual IP address (optional)	A virtual IP address to assign to the device, which can be used hide the real IP address from certain types of authorized users. (Users who have native IP access, service processor console, or device console access cannot be prevented from discovering the IP address of the dedicated Ethernet port that is connected to the OnBoard.) Virtual addresses are available only if a virtual network has been configured using DNAT. See "Why Define Virtual (DNAT) Addresses?" on page 357 for more information about when virtual addresses are needed and how the administrator creates them.
Description	A description that helps identify the device, such as IBM xSeries 306 RSA II.
Authentication type	The authentication method to be used whenever a user accesses the device. Can be different from the authentication method used for the OnBoard. See "Understanding Authentication on the OnBoard" on page 4. See also Table 1-2 on page 5 for a detailed list of authentication types supported for devices.

Caution! Be careful not to allow any PPP user to use the same IP address that is assigned to any connected device under control of the OnBoard.

Note: The OnBoard has been tested with the service processor and device types and firmware versions listed in the release notes. If the firmware on a service processor being managed by the OnBoard is at another level, or if the service processor is not listed in the release notes, the administrator needs to follow the instructions in Appendix A to configure support for the device.

Understanding Private Subnets on the OnBoard

Connected devices should be isolated (as recommended under "Understanding Device Configuration" on page 53) on a management network that is separate from the production network and from the public network. With the recommended configuration, the OnBoard administrator must create at least one private subnet for communicating with connected devices. The administrator must then assign to each connected device the following two address-related parameters:

- The name of the private subnet
- An address within the private subnet's address range to be used by devices when communicating with the OnBoard

If a device is not assigned a private subnet, the OnBoard attempts to contact the device using the default route, which cannot work unless the device is connected to a network on the public side of the OnBoard.

For more details about setting up subnets, see the following related topics.

- "Understanding Address Configuration for Connected Devices" on page 336
- "Configuring Private Subnets and Virtual Networks" on page 251

Private subnets can be configured in the Web Manager on the Wizard Subnets screen or on the Network Private Subnets screen as described in:

- "Configuring Private Subnets and Virtual Addresses—Wizard" on page 98
- "Configuring Private Subnets and Virtual Networks" on page 251.

Tasks for Configuring IP Addresses

See “OnBoard-specific Tasks for Configuring New Devices” on page 310.

Example and Demo Scripts and Application Notes

The following helps are available for OnBoard administrators:

- Configuration example scripts in `/libexec/example_scripts`
- Demo scripts in`/libexec/demo_scripts`
- Application notes in `/usr/share/docs/OnBoard/Application_Notes` with future updates to be posted at `http://www.cyclades.com/support/downloads.php` under the product name “AlterPath OnBoard.”

Understanding Data Buffering on the OnBoard

Administrators can set up storage of data from device console sessions either in local files on the OnBoard’s resident flash memory, on the hard disk of an external server, or on a PCMCIA flash memory card. When data buffering is configured, data is stored in logs under `/var/log/console/`*devicename*`.log`. The logs are rotated frequently so that the storage capacity of the OnBoard flash memory is not exceeded.

Before configuring data buffering sure that enough disk space is available to store the files in the location you select. Sequentially-written files can quickly grow to exceed the storage capacity of the local flash memory or remote hard drive. Data buffering should only be done if processes are in place to monitor the stored data.

An administrator can configure either of the two following types of data buffering:

- Global: To buffer all data from all device console sessions
- Device specific: To buffer all data from device console sessions for a specified device

The administrator can configure data buffering and log file storage only by using the `cycli` utility. See the release notes for how to configure data buffering. You can download the release notes by going to `http://www.cyclades.com/downloads.php` and searching for the product name "AlterPath OnBoard."

Understanding Firewall/Packet Filtering on the OnBoard

Packet filtering on the OnBoard is controlled by *chains* and *rules* that are configured in `iptables`. (For more details about the predefined chains and rules, see "Chains" on page 64 and "Rules" on page 64.)

Both the Web Manager and the `cycli` utility provide a way for the OnBoard administrator to add rules and to edit or delete any added rules:

- Because the OnBoard filters packets like a firewall, the Web Manager menu option under "Network" is titled "Firewall.")
- The `cycli` utility provides the `iptables` command to do the same tasks, because when rules are added, edited, or deleted, the corresponding `iptables` are updated.

By default, the OnBoard does not forward any traffic between private and public networks. The administrator might want to add rules to allow some limited communications between specific devices on the private network and the public network. For example, the administrator could add rules to allow a device to send email using an email server on the public network, as shown in the example in `/usr/share/docs/OnBoard/Application_Notes/Network/priv-to-pub.pdf`.

Caution! It is possible for an OnBoard administrator to create rules that circumvent the access controls on a device. The OnBoard administrator is responsible for understanding the implications of packet filtering rules that the administrator may add to the system and making sure that security is not compromised by the added rules.

Chains

A chain is a kind of named profile that includes one or more rules that define the following:

- A set of characteristics to look for in a packet
- What to do with any packet that has all the defined characteristics

The OnBoard comes with a number of built-in chains with hidden rules that are preconfigured to control communications between devices that are connected to the OnBoard's private Ethernet ports and devices on the public side of the OnBoard. The default chains are defined in "filter" and "nat" `iptables`. The "mangle" table is not used.

The built-in chains are named according to the type of packets they handle, as shown in the following lists. The first three chains listed below are in the `iptables` "filter" table.

- INPUT
- OUTPUT
- FORWARD

The three chains listed below are in the "nat" table. These chains implement NAT (network address translation) including the redirecting packets addressed to a virtual IP to the device's real IP address and hiding the device's real IP address when the device sends packets to the authorized user:

- PREROUTING
- POSTROUTING
- OUTPUT

Rules

Each chain can have one or more rules that define the following:

- The packet characteristics being filtered

  The packet is checked for characteristics defined in the rule, for example, a specific IP header, input and output interfaces, and protocol.

- What to do when the packet characteristics match the rule

  The packet is handled according to the specified action (called a "Rule Target," "Target Action" or "Policy").

When a packet is filtered, its characteristics are compared against the rules one-by-one. All characteristics must match.

Add Rule and Edit Rule Options

When you add or edit a rule you can define any of the options described in the following table.

Table 1-25: Filter Options for Packet Filtering Rules

Filter Options	Description
Protocol	You can select a protocol for filtering from one of the following options: • ALL • TCP • UDP • ICMP • GRE • ESP • AH
Source IP/mask **Destination IP/mask**	A host IP address or subnetwork IP address in the form: *hostIPaddress* or *networkIPaddress/NN*. If you specify a source IP, incoming packets are filtered for the specified IP address. If you specify a destination IP, outgoing packets are filtered for the specified IP address.
Input or **Output Interface**	The input or output interface used by the incoming or outgoing packet. Choices are: • Public 1 (`eth0`) • Public 2 (`eth1`) • Failover (`bond0`) • PCMCIA (`eth2`) • PCMCIA (`eth3`) • Any private port (priv0)

Table 1-25: Filter Options for Packet Filtering Rules

Filter Options	Description
Fragments	The types of packets to be filtered: • All packets and fragments • Head fragments and unfragmented packets • Non-head fragments only
Rule target	• Accept • Drop • Reject

Any of the options in Table 1-25 can be given the *inverted* flag, so that the target action is performed on packets that *do not* match any of the specified criteria. For example, if DROP is the target action, if "Inverted" is specified for a source IP address, and if no other criteria are specified in the rule, any packets arriving from any other source IP address are dropped.

Tasks for Administering Packet Filtering

Administrators can do the following tasks to specify packet filtering:

- Add new rules for existing chains
- Edit or delete administrator-added rules

The following table lists the tasks related to configuring packet filtering and where the Web Manager procedures for performing the tasks are described.

Table 1-26: Tasks for Configuring Packet Filtering (Firewall) Rules

Task	Where Documented
Add a new rule, edit or delete a customer-added rule	"Configuring Firewall Rules for OnBoard Packet Filtering" on page 239 "To Add a New Packet Filtering (Firewall) Rule" on page 241 "To Edit an Administrator-added Packet Filtering (Firewall) Rule" on page 241

The `cycli iptables` command can also be used for configuration of new rules for built-in chains.

Understanding How Configuration Changes Are Handled

The OnBoard handles *changes* to configuration files and *backups* of configuration file changes differently from how other Cyclades AlterPath products handle them. The following bulleted items give an overview of how the OnBoard handles configuration changes:

- When an OnBoard administrator performs configuration tasks, changes are stored in RAM memory until the administrator takes a specific action to save the changes in configuration files.
- Unless changes are saved in configuration files, they do not persist after a reboot.
- The OnBoard administrator can back up changed configuration files at any time.
- Like other AlterPath products, the OnBoard maintains a backed up copy of the factory-default configuration files.
- The OnBoard administrator can restore the factory default files or restore any backed-up copies of the configuration files that an administrator may make during system operation.
- The current state of the configuration files is maintained after a software upgrade. (This allows you to upgrade software on the OnBoard without losing all user and device configurations.) After a software upgrade, the administrator can optionally do the following:
  - Return to the last backed-up copy of the configuration files.
  - Return to the factory default configuration files.

Saving Configuration Changes

The following table shows how administrators can save changes to configuration files in different environments on the OnBoard.

Table 1-27: Options for Saving Configuration File Changes

Environment	Action
Web Manager	On any Web Manager screen while logged in as an administrative user, click the "Save and apply changes" button. (When changes are made using the Web Manager, an "Unsaved changes" button displays until the administrative user clicks the "Save and apply changes button.")
OnBoard `cycli` utility	Invoke the `cycli` utility using the `-C` option or enter the `commit` command before quitting `cycli`.

Backing Up Configuration File Changes

The following table shows how administrators can back up configuration files in different environments on the OnBoard. When the administrator performs one of the actions shown in Table 1-28, the system creates a compressed backup of all the configuration files and stores it in `/mnt/hda3/backup/configuration_files.gz`. Any compressed configuration file that already resides in the directory is overwritten.

Table 1-28: Options for Saving Configuration File Changes

Environment	Action
Web Manager	While logged in as an administrative user, go to the Mgmt → Backup/restore screen and click the "Save" button.
OnBoard Linux command line	Enter the `saveconf` command

Restoring Backed Up Configuration Files

The administrator can restore backed-up changes to configuration files that have been stored in the `configuration_files.gz` file by performing the actions shown in the following table.

Table 1-29: Options for Saving Configuration File Changes

Environment	Action
Web Manager	While logged in as an administrative user, go to the Mgmt → Backup/restore screen and click the "Load" button.
Command line	Enter the `restoreconf` command followed by the `sync` command.

Restoring Factory Default Configuration Files

A compressed copy of the factory default configuration files is stored in the the `/mnt/hdCnf/backup` directory as `factory_default_files.gz` for possible restoration at any time.

The administrator can restore the factory default configuration files from the `factory_default_files.gz` file by performing the actions shown in the following table.

Table 1-30: Options for Saving Configuration File Changes

Environment	Task	Action
Command line	Restoring factory defaults on the Linux command line	Enter the `restoreconf factory_default` command followed by the `sync` command
	Saving an image to compact flash and restoring the factory defaults	Enter the `create_cf` command with the `--factory_default` option.
U-boot monitor mode	Booting from the network and using the factory default configuration.	Enter the `net_boot configsource=factory_default` command.

Configuring Files to Be Backed Up and Restored

The `/etc/config_files` file lists all files to be backed-up and restored, including its own filename.

If you add a file or a script to the system, make sure to add the file's pathname to the `config_files` file.

▼ To Configure an Added Script or Other File for Backup and Restoration

1. Log into the OnBoard command line as root.
2. Change to the `/etc` directory.

```
[root@OnBoard /] cd /etc
```

3. Open the `config_files` file for editing.

```
[root@OnBoard /] vi config_files
```

4. Add the pathname of the new file to the list.

```
/etc/ypbind.conf
/etc/yp.conf
/etc/localtime
/etc/timezone
/pathname/to/new/file
```

5. Save and quit the file.

```
:wq
```

Task for Restoring Configuration Files

The following table provides links to where the tasks and options for restoring configuration files are described.

To Restore the OnBoard Configuration Files to the Last Saved Version	Page 380
To Restore the OnBoard Configuration Files to the Factory Defaults	Page 381
Options for the create_cf Command	Page 381
Options for the restoreconf Command	Page 384

Chapter 2
Web Manager Introduction

This chapter provides an overview of the Web Manager features for the administrative user.

The information is provided in the following sections.

Logging Into the Web Manager	Page 74
Features of Administrator's Screens	Page 77
Overview of Web Manager Menus	Page 79

This chapter provides the procedures listed in the following table.

To Log Into the Web Manager	Page 75
To Disable Web Manager Timeouts	Page 76

Logging Into the Web Manager

Two types of administrative users can access all the Web Manager functions described in this guide:

- An administrator who knows the password for the “admin” account, which is configured by default
- An optionally-added regular user whose account is in the “admin” group

For more details about the differences between user types, see “Types of Users” in the *AlterPath OnBoard User’s Guide*.

OnBoard administrative users, like regular users, can access the Web Manager from a browser using HTTP or HTTPS either over the Internet or through a dial-in or callback PPP connection.

Like regular users, administrative users can use default menu options that appear on the first Web Manager screen after login to do the following:

- Access devices
- Manage power
- Change their own passwords

How to perform the tasks in the above list is described in the *AlterPath OnBoard User’s Guide*.

In addition to being able to perform all the tasks regular authorized users can perform, administrative users can use the Web Manager for configuring users, devices, and other OnBoard features that enable the enforcement of the organization’s security policies.

Only one administrative user can connect to the Web Manager at a time. The message shown in the following screen example appears if an another administrative user is currently logged in. The dialog provides the option either to cancel the current login attempt or to log out the currently-logged-in administrative user.

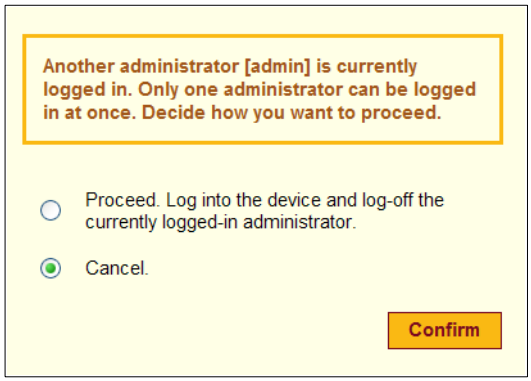


Figure 2-1: Web Manager Message When An Administrative User is Already Logged In

In the *AlterPath OnBoard User's Guide*, see "Cyclades Web Manager" for background about the Web Manager and "Prerequisites for Using the Web Manager" for the required browsers, preparation, and browser plug-ins.

▼ *To Log Into the Web Manager*

This procedure assumes you know the admin password or the username and password for an administrative user account and that you have one of the following types of access to the OnBoard:

- A network connection to the OnBoard
- A dialup connection over a phone line

1. Enter the IP address of the OnBoard in a supported browser.

   Refer to the *AlterPath OnBoard User's Guide* for a list of supported browsers, if needed.

   The Web Manager login screen appears.

2. Enter the username and password.
3. Click the "Login" button.

▼ To Disable Web Manager Timeouts

This procedure requires an administrator who knows the root password and who is able to log into the OnBoard console to manually change the timeout value by editing a configuration file. The default timeout value is 1800 seconds (30 minutes). The value can be changed to any number of seconds up to 2^{13}, up to sixty years.

1. Connect to the OnBoard's console and log in as root.
2. Change to the `/etc/cacpd` directory and open the `cacpd.conf` file for editing.
3. Find the following lines:

```
config{
        timeout: 1800
}
```

4. Change the timeout value to the desired number of seconds.
5. Save and quit the file.
6. Either restart the OnBoard or enter `killall cacpd` on the command line, as shown in the following screen example.

```
[root@onboard etc/cacpd]# killall cacpd
```

Features of Administrator's Screens

The following figure shows features of the Web Manager that appear when an administrative user logs in.

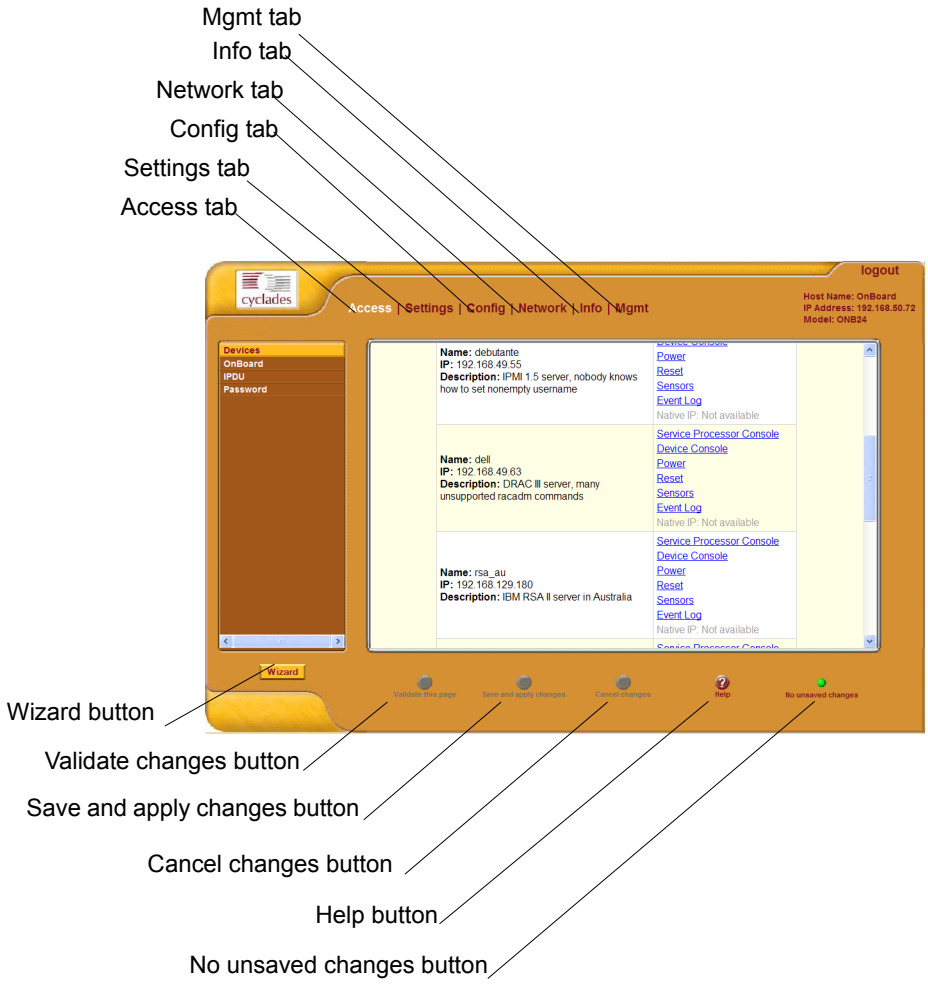


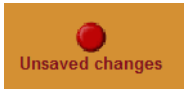
Figure 2-2: Administrative User Options on the Web Manager

Selecting an item from the top menu changes the list of menu options displayed in the left menu.

An option in the left menu (such as "IPDU" in the Figure 2-2) often has several related screens associated with it. The related screens are accessed as tabs. Selecting a tab brings up the related screen.

The following table describes the six additional buttons that appear at the bottom of the administrative user's screen that are not available for a regular user.

Table 2-1: Buttons That Display Only for Administrative Users

Button Name	Description
Wizard	Displays the configuration wizard. See Chapter 3, "Web Manager Wizard.
Validate this page	Checks for errors in user entries without updating configuration files.
Save and apply changes	Saves all the changes made to the configuration and causes the OnBoard to start using the new settings.
Cancel changes	Returns the configuration of the OnBoard to the state it was in right after the last time the "Save and apply changes" button was pressed.
No unsaved changes	A green button appears with this label when no unsaved changes exist.
Unsaved changes	A red button blinks above this label when unsaved changes exist.
	

Dialogs are screens that appear when an administrative user clicks an "Add" or "Edit" button. While dialogs are active, the buttons at the bottom of the screen, which are listed in Table 3-1, and the menu options are grayed out. The appearance of an active dialog is shown the following screen example. The grayed out options and buttons become active only after the administrative user clicks either the "OK" or "Cancel" button. The administrative user may need to click other types of buttons to exit other types of dialogs.

Figure 2-3: Example Dialog: Devices Configuration—in Wizard Mode

Overview of Web Manager Menus

The following figure shows all the top and left menu options available to the administrative user.

- **Access**
  - Devices
  - OnBoard
  - IPDU
  - Password
- **Settings**
  - AUX port
  - IPDU
  - PCMCIA
  - Date/time
  - Boot configuration
  - Help
- **Config**
  - Devices
  - Users and groups
  - Authentication
  - Unit authentication
  - Notifications
  - Sensor alarms
  - SNMP
  - Syslog
  - Event log backend
  - Security profile
  - Services
- **Network**
  - Host settings
  - Firewall
  - Host table
  - Static routes
  - VPN connections
  - Outbound email
  - Private subnets
- **Info**
  - Session status
  - System information
  - Detected devices
- **Mgmt**
  - Backup / restore
  - Firmware upgrade
  - Restart

The left menu options are described in the following chapters:

- Chapter 4, “Web Manager “Access” Menu Options”
- Chapter 5, “Web Manager “Settings” Menu Options”
- Chapter 6, “Web Manager “Config” Menu Options”
- Chapter 7, “Web Manager “Network” Menu Options”
- Chapter 8, “Web Manager “Info” and “Mgmt” Menu Options”

Chapter 3
Web Manager Wizard

This chapter describes how an administrative user can use the Wizard to perform basic configuration.

For an overview of all the Web Manager features and menu options that are available for administrative users, see Chapter 2, “Web Manager Introduction,” if needed.

This chapter covers the topics in the following sections.

Using the Wizard	Page 82
Changing the Administrative User’s Password—Wizard	Page 84
Selecting a Security Profile—Wizard	Page 85
Configuring Network Interfaces—Wizard	Page 91
Configuring Private Subnets and Virtual Addresses—Wizard	Page 98
Configuring Devices—Wizard	Page 104
Configuring Regular Users —Wizard	Page 107

This chapter provides the procedures listed in the following table.

To Change the Administrative User’s Password—Wizard	Page 85
To Select or Configure a Security Profile—Wizard	Page 91
To Configure OnBoard Network Interfaces—Wizard	Page 96
To Create and Authorize a User for Device Management—Wizard	Page 108

Using the Wizard

The Wizard screen displays a list of options in the left menu, as shown in the following figure. An administrative user can use the menu options to perform basic configuration of the OnBoard.

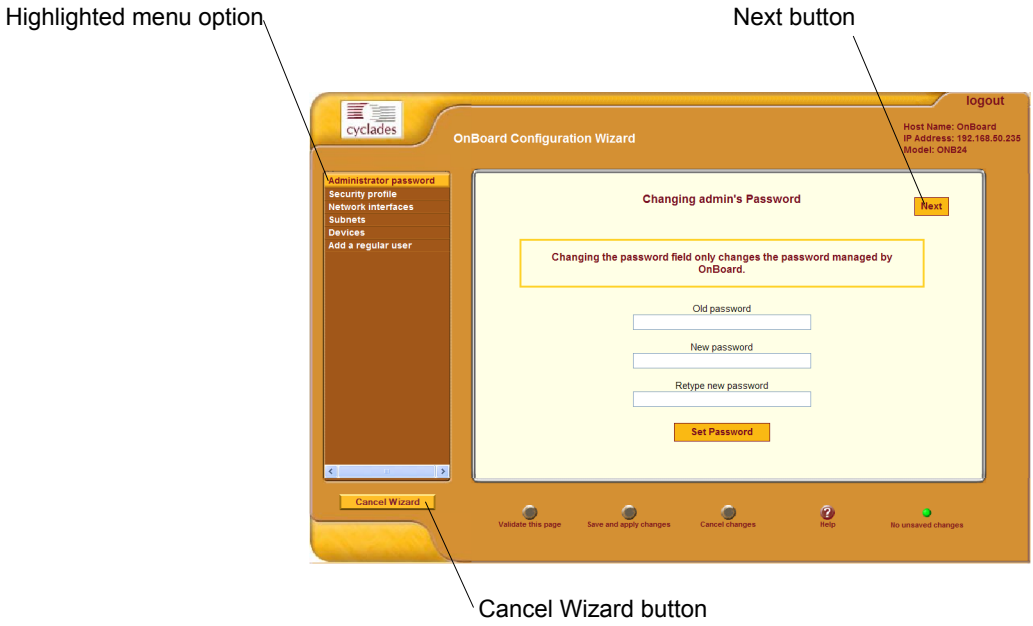


Figure 3-1: Wizard Screen

The “Cancel Wizard” button shown in Figure 3-1 appears only in Wizard mode. A “Next” button appears on all Wizard pages in a series except the last. A “Previous” button (shown in Figure 3-3) appears on all pages in a series except the first. When a Wizard configuration option includes a series of related screens, clicking the “Previous” and “Next” buttons brings up the previous and next screens in the series.

If the administrative user clicks the “Cancel Wizard” button after making changes but before saving the changes, a dialog appears as shown in Figure 3-2.

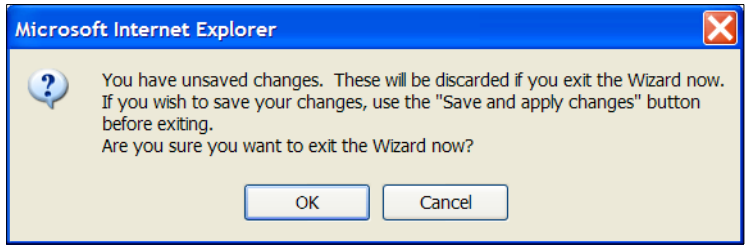


Figure 3-2: "Cancel Wizard" Button Dialog

The dialog shown in Figure 3-2 offers the following choices:

- Press the "Cancel" button to return to the Wizard, where the administrative user can click the "Save and apply changes" button to save the changes before cancelling the Wizard again.
- Press "OK" to exit the Wizard and lose any unsaved changes.

After the "Next" button is clicked on the last screen of the Wizard, the screen shown in the following figure appears. Clicking the "Next" button on this screen saves all changes made on any of the Wizard screens.

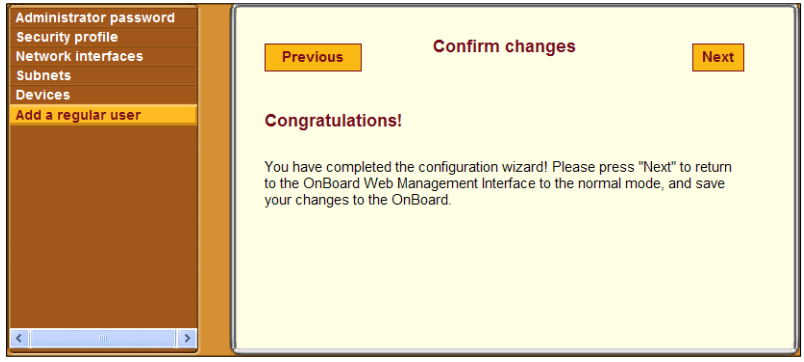


Figure 3-3: Wizard "Confirm Changes" Screen

The following table lists the tasks the administrative user can perform using the Wizard with links to where the tasks are described.

Table 3-1: Wizard Steps and Where They are Described

Wizard Step	Where Described
Change the administrative user's password	"Changing the Administrative User's Password—Wizard" on page 84
Select an OnBoard security profile	"Selecting a Security Profile—Wizard" on page 85
Configure network interfaces	"Configuring Network Interfaces—Wizard" on page 91
Configure subnets	"Configuring Private Subnets and Virtual Addresses—Wizard" on page 98
Configure devices	"Configuring Devices—Wizard" on page 104
Configure regular users	"Configuring Regular Users —Wizard" on page 107

Changing the Administrative User's Password—Wizard

Figure 3-4 shows the screen that appears when the "Administrator password" option is selected from the Wizard menu.

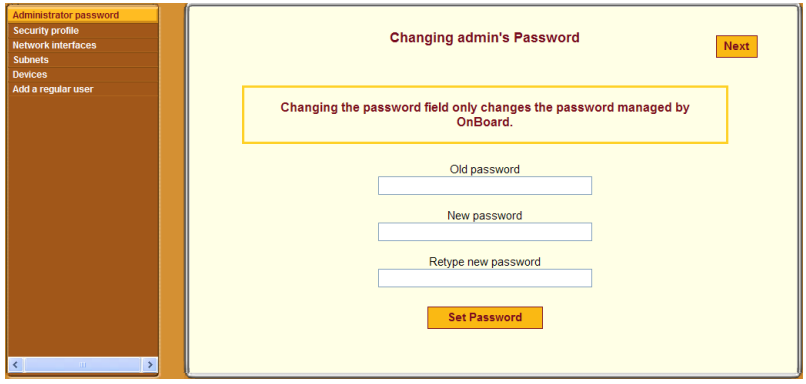


Figure 3-4: Wizard "Configure Administrator Password" Screen

Caution! If the default password “cyclades” is still in effect, changing the password now is essential to reduce the risk of intrusion. Leaving the password unchanged leaves a security breach that makes all connected equipment vulnerable.

▼ *To Change the Administrative User’s Password—Wizard*

1. Log into the Web Manager as an administrative user.

   See “To Log Into the Web Manager” on page 75, if needed.

2. Click the “Wizard” button.

   The “Administrator Password” option is highlighted and the “Configure Administrator Password” screen is active by default.

3. Enter a new password for the administrative user in the “Password” field and retype it in the “Retype password” field.

4. Click the “Set Password” button to save the password.

Selecting a Security Profile—Wizard

Figure 3-1 shows the screen that appears when the “Security profile” option is selected from the Wizard menu. The screen identifies the name of the security profile currently in effect. For more details about the services and features configured by default security profiles and what you can change in a custom profile, see “Understanding Security Profiles” on page 12.

As stated in the note at the bottom of the security profile configuration screen, putting another security profile into effect could disable or enable services that may have been turned on or off by some other means. For more details, see “Understanding Services on the OnBoard” on page 17.

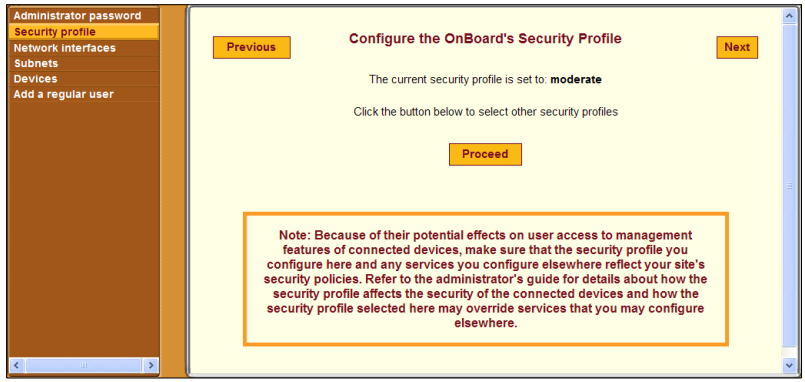


Figure 3-5: Config → Security Profile Screen With the "Moderate" Profile Enabled

Clicking the "Proceed" button on the Security Profile Caution screen brings up the Security Profile configuration dialog shown in the following figure.

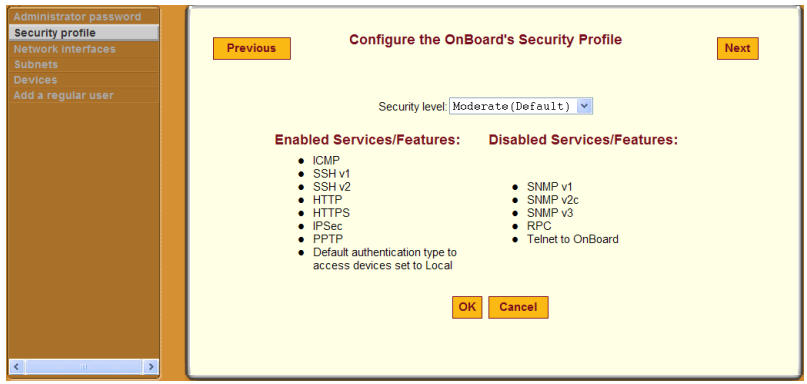


Figure 3-6: Security Profile Configuration Dialog With "Moderate" Profile Selected

An administrative user can use the dialog shown in Figure 3-6 to select one of the default security profiles or configure a custom security profile for the OnBoard. See "Understanding Security Profiles" on page 12 for important background information.

The Moderate profile is the default option selected on the "Security level" menu. The features in the "Moderate" security profile are described in Table 1-6, "Moderate Security Profile Services/ Features," on page 12.

After the administrative user chooses a preconfigured security profile or creates a custom profile and clicks “OK,” the red “Unsaved changes” button blinks, and the Security Profile screen reappears showing the newly-selected security profile’s name. The following figure illustrates the screen after the security profile’s name is changed to “secured,” and the red “Unsaved changes” light is lit. The administrative user must click the “Save and apply changes” button to put the newly selected profile into effect.

Figure 3-7: Security Profile Confirmation Screen

Secured

The following figure shows the lists of enabled and disabled features in the dialog for the “Secured” security profile.

Figure 3-8: Secured Profile Dialog

Note: Follow the reminder at the bottom of the screen shown in Figure 3-8 by making sure to notify all users that they must use HTTPS when bringing up the Web Manager, because HTTP is disabled by the secured security profile.

The features in the “Secured” security profile are described in Table 1-7, “Secured Security Profile Services/Features,” on page 13.

Open

The following figure shows the lists of enabled and disabled features in the dialog for the “Open” security profile.

Figure 3-9: Open Security Profile Dialog

The features in the “Open” security profile are described in Table 1-8, “Open Security Profile Services/Features,” on page 13.

Custom

The following figure shows the features that can be enabled and disabled in the dialog for the “Custom” security profile.

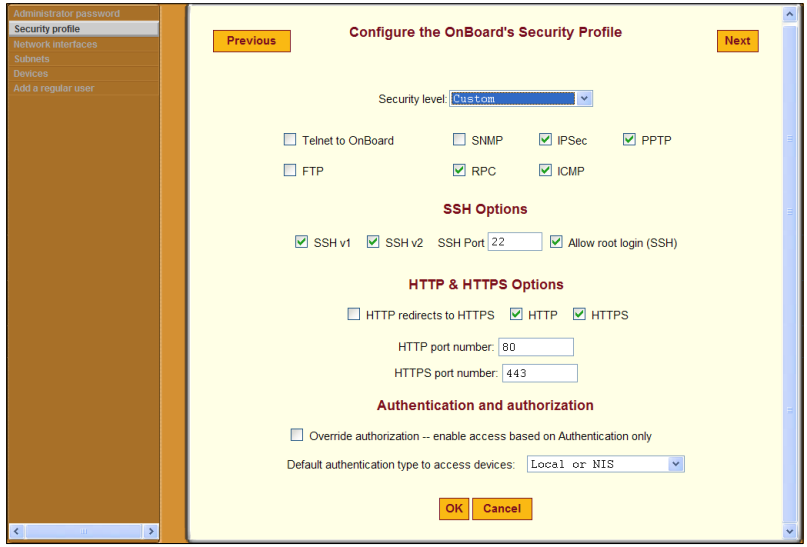


Figure 3-10: Custom Security Profile Dialog

The options that can be configured in a custom security profile are described in Table 1-9, “Services and Other Functions in the “Custom” Security Profile,” on page 14.

Note: Selecting a default authentication type means that the specified authentication type is selected by default in the Web Manager when a new device is being configured, and the default authentication type is also assigned by default to a new device that is configured using the `cycli` utility after the profile goes into effect. The administrative user can change the authentication type for each individual device while configuring it.

▼ *To Select or Configure a Security Profile—Wizard*

1. Log into the Web Manager as an administrative user.

   See “To Log Into the Web Manager” on page 75, if needed.

2. Click the “Wizard” button.

   Click the “Security profile” option in the left menu bar.

3. Click the “Proceed” button.

4. Select a security profile from the “Security Level” pull-down menu.

5. If you select the “Custom” profile, make sure the checkboxes are checked next to services and features you want to be enabled and make sure the checkboxes are clear next to services and features you want to be disabled.

6. Click “OK.”

   The security profile confirmation screen appears.

7. Click the “Save and apply changes” button.

8. Click the “Next” button, if desired, to go to the next Wizard step.

Configuring Network Interfaces—Wizard

Figure 3-1 shows the first of a series of related screens that appears when the “Network interfaces” option is selected from the Wizard menu.

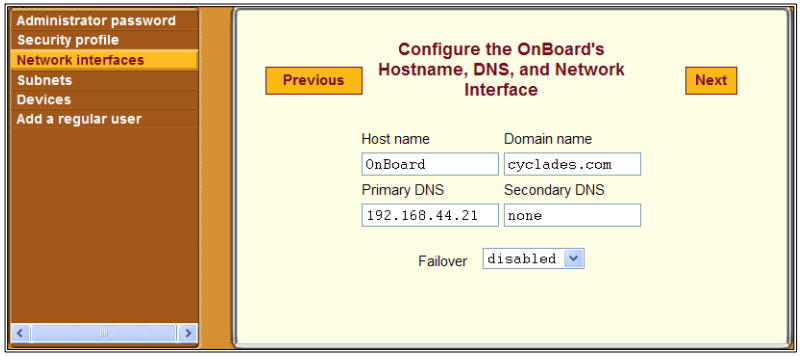


Figure 3-11: Network Interfaces Screen—Wizard

The screen shown in Figure 3-11 allows the administrative user to set or change the parameters in the following table.

Table 3-2: Network Interfaces Configuration Values

Settings	Notes
Host name	Default: OnBoard
Domain name	Domain name used on the domain name server (DNS)
Primary DNS server	IP address for a primary DNS server on the same subnet as the OnBoard
Secondary DNS server	IP address for an optional secondary DNS server on the same subnet as the OnBoard
Failover	Selecting “enabled” from the pull-down menu configures failover from the primary to the secondary Ethernet port if the primary port goes down. For background information, see “Understanding Ethernet Ports on the OnBoard” on page 41.

Clicking the “Next” button on the “Network Interfaces” screen brings up one of two screens, depending on whether failover is enabled or disabled. See “Configuring Failover” on page 94 and “Configuring Primary and Secondary Ethernet Ports” on page 94.

Table 3-3 describes the parameters that can be set on the failover configuration screen, and on the primary and secondary Ethernet configuration screens.

Table 3-3: Ethernet Port Settings

Settings	Notes
DHCP	DHCP is enabled by default on the OnBoard's interfaces. If DHCP is enabled, the OnBoard looks for a DHCP server on the same network. If a DHCP server cannot be located, the OnBoard falls back to using the default IP address described below. The additional fields in the table rows below appear only if DHCP is not checked, because they are needed only when configuring a static IP address for the interface.
IP address	192.168.160.10 is assigned by default to eth0.
Network mask	The desired netmask in the form: 255.255.255.0.
Gateway IP	IP address for a gateway on the same subnet as the OnBoard
MTU	The maximum transmission unit value for the Ethernet port. Default=1500.
Broadcast IP	The reserved broadcast IP address.

Configuring Routes

Configuring the network interfaces sets up a default route for the OnBoard. When the DHCP checkbox is checked on any of the network interface screens, the DHCP server assigns the OnBoard a default route. If the DHCP checkbox is not checked, the gateway IP specified by the administrative user in the "Gateway IP" field is used to create a default route for the interface. If a host or network route is required, the administrative user should go to the Network → Static routes screen.

Configuring Failover

If failover is enabled on the “Network Interfaces” screen, clicking the “Next” button brings up a screen for configuring the failover device. The following figure shows the fields that appear on the screen for configuring the failover device if the DHCP option is not checked. If the DHCP option is not checked, no further configuration is needed. Clicking the “Next” button brings up the subnet configuration screen.

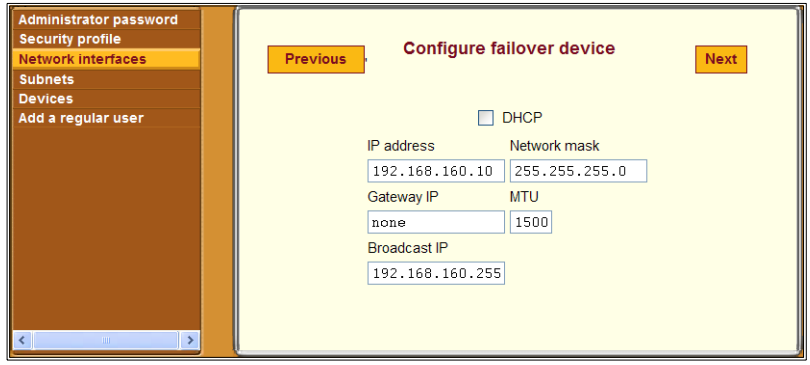


Figure 3-12: “Configure Failover Device” Screen

With failover enabled, the secondary Ethernet interface becomes bonded to the primary Ethernet interface, and the secondary Ethernet interface becomes active only if the primary Ethernet port is not available. As a result, the values entered in the fields on the screen shown in Figure 3-12 apply to the single bond0 interface.

Configuring Primary and Secondary Ethernet Ports

If failover is disabled, the administrative user can configure each Ethernet port separately in the following ways:

- Enable or disable each Ethernet port
- Enable or disable DHCP
- If DHCP is disabled, configure each port for static IP addressing.

When failover is disabled on the “Network Interfaces” screen, clicking the “Next” button brings up the first of two screens for configuring the primary and secondary Ethernet ports. The screen for configuring the secondary Ethernet port is identical to the screen for the primary Ethernet port except for the screen’s heading. The screen for configuring the primary Ethernet port is

shown in the following figure as it appears when the “Enable” checkbox is not checked.

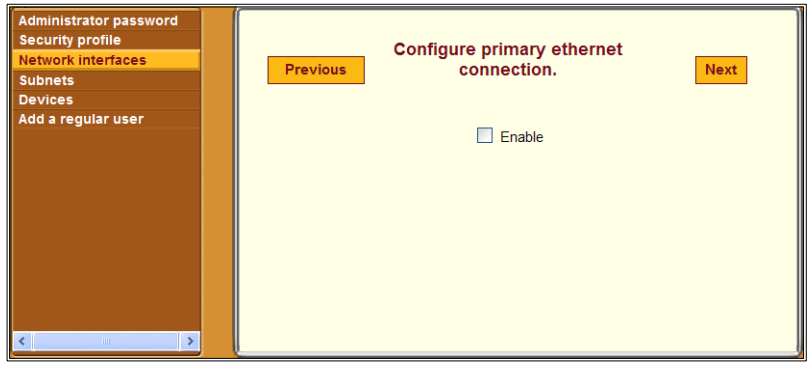


Figure 3-13: “Configure Primary Ethernet Connection” Screen

Figure 3-14 shows the screen for configuring the primary Ethernet port as it appears when both the “Enable” and “DHCP” checkboxes are checked.

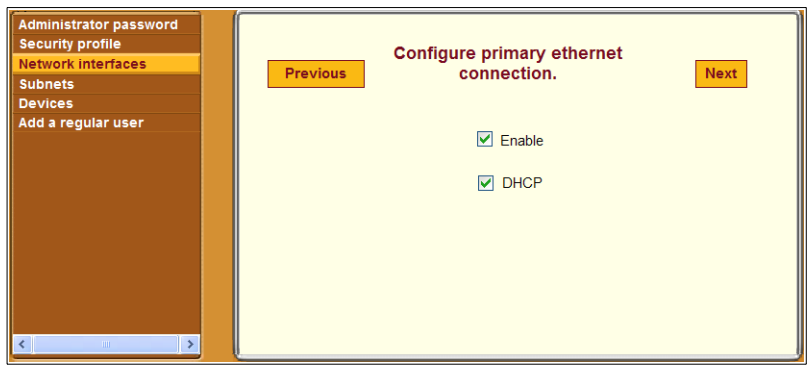


Figure 3-14: “Configure Primary Ethernet Connection:” Enabled With DHCP

Figure 3-15 shows the screen for configuring the primary Ethernet connection with the additional fields that appear when the “DHCP” button is not checked. The administrative user enters the required information on this screen for configuring the OnBoard to use a static IP address.

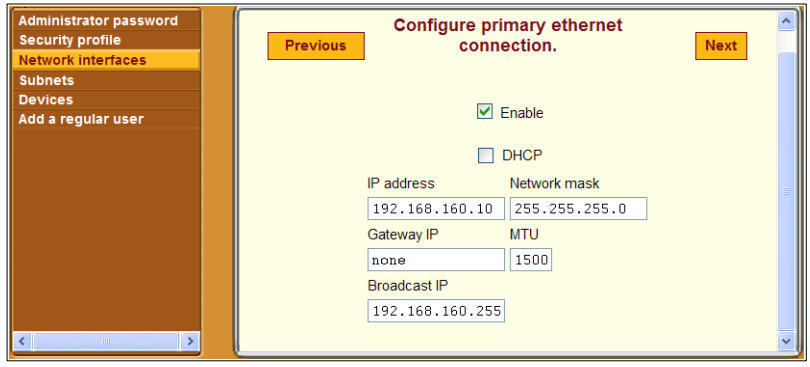


Figure 3-15: "Configure Primary Ethernet Connection" Screen: Static IP

Clicking the "Next" button on the primary Ethernet configuration screen brings up a screen for configuring the secondary Ethernet connection. Clicking the "Next" button on the secondary Ethernet configuration screen brings up the next Wizard screen for configuring subnets.

▼ *To Configure OnBoard Network Interfaces—Wizard*

1. Log into the Web Manager as an administrative user.

   See "To Log Into the Web Manager" on page 75, if needed.

2. Click the "Wizard" button.

   Click the "Network interfaces" option in the left menu bar.

3. Modify the name in the "Host name" field, if desired.
4. Enter or modify an existing DNS domainname in the "Domain name" field.
5. Enter or modify the IP address for a primary DNS server into the "Primary DNS" field.
6. Enter or modify the IP address for a secondary DNS server in the "Secondary DNS" field.
7. Enable or disable failover by selecting the desired option from the "Failover" pull-down menu.

8. Click the “Next” button.
   - If failover is disabled, clicking the “Next” button brings up the first of two screens for configuring the primary and secondary Ethernet ports.

Note: Connecting the secondary Ethernet port to a separate network and assigning a separate IP address is optional, so you can skip the screen for configuring the secondary Ethernet port, if desired.

   - If failover is enabled, clicking the “Next” button brings up a screen for configuring the failover device.

Note: Whether you are configuring failover or configuring the primary and secondary Ethernet ports separately, the fields are the same.

---

9. If desired, enable DHCP on any of the network interface configuration screens, by clicking the “DHCP” checkbox.
10. If desired, configure the selected Ethernet port to use a static IP address by performing the following steps.
    a. Disable DHCP by making sure the “DHCP” checkbox is not checked.
    b. Enter or modify the IP address in the “IP address” field.
    c. Enter or modify the netmask in the “Network mask” field.
    d. Enter or modify the IP address for a network gateway in the “Gateway IP” field.
    e. Enter or modify the maximum transmission unit value for the Ethernet port in the “MTU” field.
    f. Enter or modify the broadcast IP address for the Ethernet port in the Broadcast IP field.
11. If failover is disabled, and the current Ethernet port is the primary Ethernet port, click the “Next” button and perform Step 10 again on the secondary Ethernet port configuration screen for the secondary Ethernet port, if desired.
12. Click “Save and apply changes.”
13. Click the “Next” button, if desired, to go to the next Wizard step.

Configuring Private Subnets and Virtual Addresses—Wizard

Figure 3-16 shows the “Configure subnets” screen that appears when the administrative user selects the “Subnets” option from the Wizard menu.

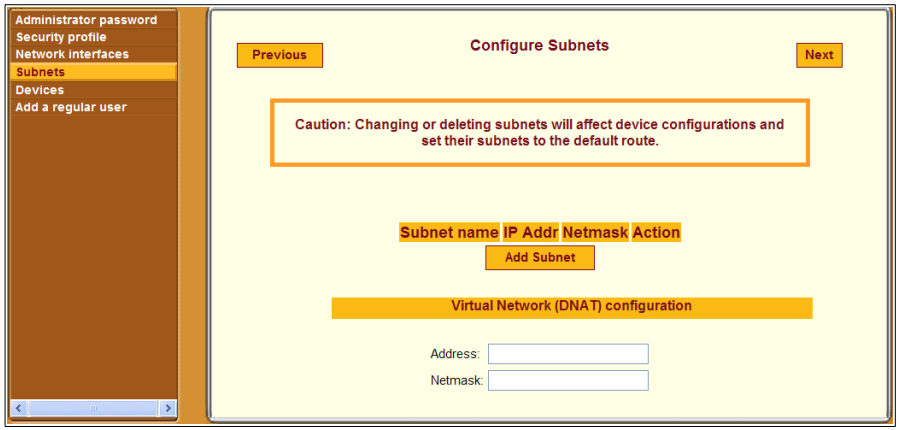


Figure 3-16: “Configure Subnets” Screen—Wizard

Caution! Changing or deleting an existing private subnet changes the configuration of any device that was previously-configured to use that private subnet; the private subnet is removed from the device’s configuration, and on subsequent attempts to contact the device, the OnBoard tries to use the default route. After changing or deleting a private subnet, to avoid making devices unavailable make sure to reassign all affected devices to the correct private subnet.

Before configuring and assigning private subnets, the site’s administrators must plan an addressing scheme that reflects the needs of the organization. Configuring private subnets is only part of the preparatory work that must be done.

See “Understanding Device Configuration” on page 53 and “Understanding Private Subnets on the OnBoard” on page 61 for an introduction to the information needed for understanding what private subnet(s) you need to configure and what values to enter in the fields shown in Figure 3-17. See also Appendix , ‘Advanced Device Configuration” on page 309.

On this screen, the administrative user can also configure a virtual network based on Destination Network Address Translation (DNAT).

See the following sections for more details:

- “Configuring Private Subnets” on page 99
- “Configuring a Virtual Network” on page 102

Configuring Private Subnets

Clicking the “Add Subnet” button on the “Configure Subnets” screen brings up the “Private Subnet configuration” dialog shown in the following screen example.

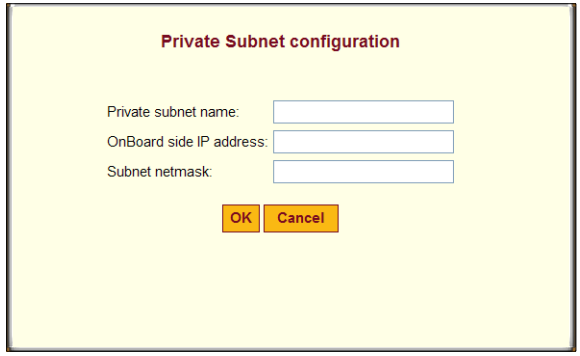


Figure 3-17:“Configure Subnets” Screen—Wizard: Add Subnet Dialog

At least one private subnet must be defined to enable devices that are connected to the OnBoard’s private Ethernet ports to communicate over the Internet via the OnBoard’s public IP address. Any number of private subnets may be configured.

The following table defines the information that the administrative user must supply in the fields that define a subnet.

Table 3-4: Fields on the Private Subnet Configuration Dialog

Field	Definition
Private subnet name	Any meaningful name chosen by the administrator.
OnBoard side IP address	Devices use this address when communicating with the OnBoard. The OnBoard uses this address when communicating with devices. This address must be within the private subnet's IP address range.
Subnet mask	Defines the range of addresses available on the subnet.

The OnBoard derives the range of addresses in the subnet from the OnBoard-side IP address and the subnet mask.The OnBoard uses the specified information to create a route to the subnet in the OnBoard's routing table.

The example in Figure 3-18 shows a private subnet name of "net1," an OnBoard side IP address of 192.168.0.254, and a subnet netmask of 255.255.255.0. The private subnet address derived from this configuration is 192.168.0.0.

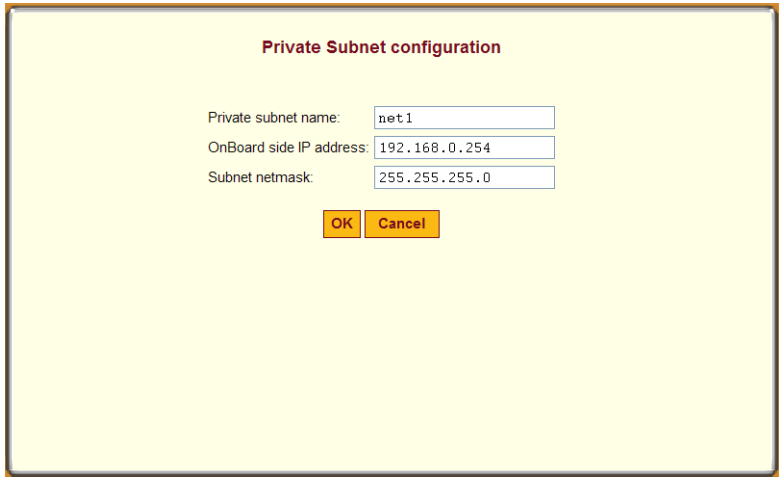


Figure 3-18: Network → Private Subnets: Add Subnet Dialog

Since the broadcast address in the example is 192.168.0.255 (by convention) and the OnBoard's address is 192.168.0.254, the administrator can assign an IP address out of the remaining available IP addresses between 192.168.0.1 and 192.168.0.253 when configuring a connected device.

Multiple private subnets may be needed if IP addresses are already assigned to connected devices' Ethernet ports and if the IP addresses are not in the same range.

▼ *To Add a Private Subnet—Wizard*

1. Log into the Web Manager as an administrative user.

   See "To Log Into the Web Manager" on page 75, if needed.

2. Click the "Wizard" button.
3. Click the "Subnets" option in the left menu bar.
4. Click the "Add Subnet" button.
5. Enter a meaningful name for the private subnet in the "Private subnet name" field.
6. Enter an IP address within the private subnet's network address range in the "Onboard side IP address" field.
7. Enter a netmask for the subnet in the "Subnet netmask" field.
8. Click OK.
9. Click "Save and apply changes."
10. Click the "Next" button, if desired, to go to the next Wizard step.

▼ *To Edit a Private Subnet—Wizard*

1. Log into the Web Manager as an administrative user.

   See "To Log Into the Web Manager" on page 75, if needed.

2. Click the "Wizard" button.
3. Click the "Subnets" option in the left menu bar.
4. Click the "Edit" button for the entry for the private subnet you want to change.

5. Accept or change the name of the private subnet in the “Private subnet name” field.
6. Accept or change the IP address in the “Onboard side IP address” field.
7. Accept or change the netmask for the subnet in the “Subnet netmask” field.
8. Click OK.
9. Click “Save and apply changes.”
10. Click the “Next” button, if desired, to go to the next Wizard step.

Configuring a Virtual Network

A virtual network based on Destination Network Address Translation (DNAT) must be defined in the following cases:

- When multiple *subnets* must be supported (as when connected devices are previously configured with IP addresses from multiple address ranges, and it is not feasible to change the already-defined device IP addresses and the administrator does not what users to be required to set up a separate route to each subnet from their workstations)
- When it is important to hide the addresses of connected devices from users by the use of *virtual IP addresses*

Figure 3-16 shows the fields for configuring a virtual network with DNAT, which appear on the “Configure Subnets” Wizard screen.

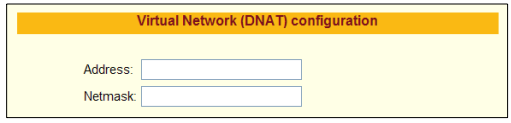


Figure 3-19: “Configure Subnets” Screen: Virtual Network (DNAT) Configuration

The following table defines the information that must be supplied in the fields that define a virtual network:

Table 3-5: Fields on the Private Subnet Virtual Network Configuration Dialog

Field	Description
Address	IP address to assign to the OnBoard from the virtual network. For example, if the virtual IP address of the network is 10.0.0.0, 10.0.0.254 would a valid IP address for the OnBoard that could be entered here.
Netmask	Netmask (which is used in combination with the network address portion of the "Address" above to define the address range of the virtual network), in the form *NNN.NNN.NNN.N*, as in: 255.255.255.0.

▼ *To Configure a Private Subnet and Optional Virtual Network—Wizard*

1. Log into the Web Manager as an administrative user.

   See "To Log Into the Web Manager" on page 75, if needed.

2. Click the "Wizard" button.
3. Click the "Subnets" option in the left menu bar.
4. Under "Virtual Network (DNAT) configuration," enter the IP address within the virtual network's network address range in the "Address" field.
5. Enter a netmask in the "Netmask" field.
6. Click "Save and apply changes."
7. Click the "Next" button, if desired, to go to the next Wizard step.

Configuring Devices—Wizard

Figure 3-16 shows the “Configure devices” screen that appears when the “Devices” option is selected from the Wizard menu. As shown, entries appear for the each configured device, and “Edit” and Delete” buttons appear next to each device’s entry. The “Add new device” button always appears on the screen.

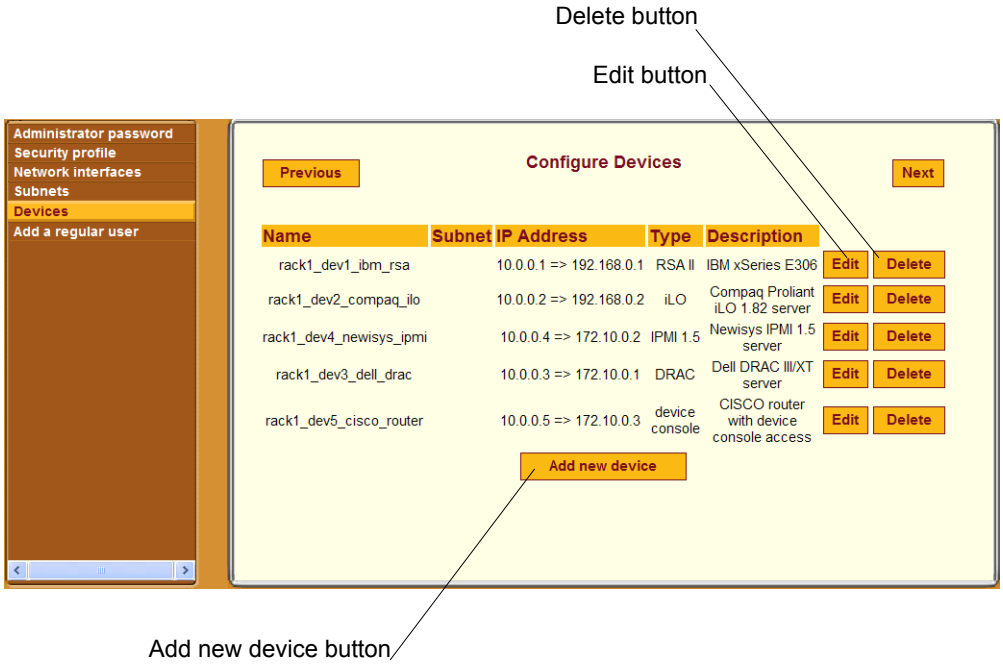


Figure 3-20: “Configure Devices” Screen—Wizard

Clicking the “Add new device” button brings up the dialog shown in the following figure, which can be used to configure a new or previously-added device. The screen that appears when “Edit” is selected for a device has the same fields as the “Add new device” screen.

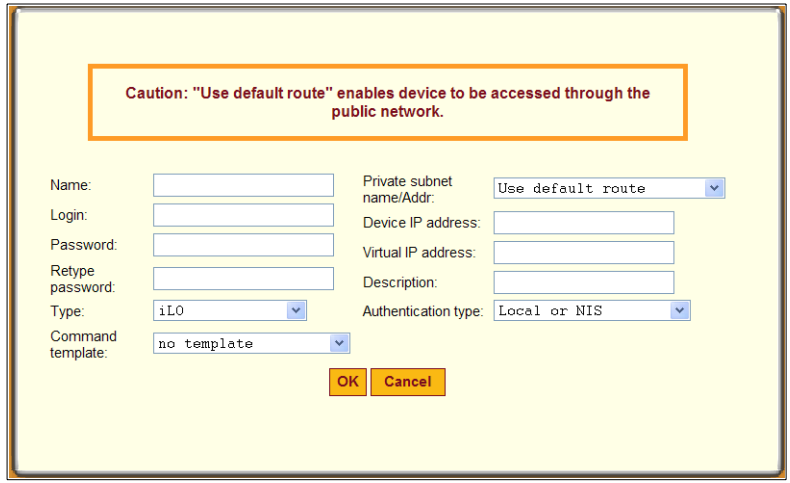


Figure 3-21: "Add New Device" Dialog—Wizard

Caution! All devices connected to the private Ethernet ports of the OnBoard must have a previously-configured private subnet name assigned. The Caution at the top of the dialog shown in Figure 3-21 is a reminder that if the default route is assigned, the device could only be accessed if it is connected to the public interface of the OnBoard, a highly unlikely scenario and not recommended.

Table 1-24, "Device Configuration Parameters," on page 58 lists the parameters that must be configured for each device.

Clicking the "Next" button brings up a screen for configuring a regular user.

Device Types

The following lists each of the defined service processor and device types.

- iLO
- RSA II
- DRAC
- IPMI 1.5
- device console

Three additional custom types may be assigned, but only if OnBoard administrators have created customized scripts:

- `custom1`
- `custom2`
- `custom3`

Note: In most cases, the administrative user should not assign custom device types. Assign a `custom`*N* type only if the default scripts and command templates cannot be made to work and only if an OnBoard administrator has created a custom expect script with the same number in its name. For details, see Appendix A, "Advanced Device Configuration."

Command Templates

As mentioned elsewhere in this document, command templates contain text commands that are used to interact with connected service processors/devices.

The following table lists the default command templates and describes the types of devices to which they apply. See "Understanding How the OnBoard Manages Communications With Devices" on page 311" for how to test the default command templates, and what to do if they do not work.

Table 3-6: Default Command Templates

Template	Type of Device
`devconsole.default`	Devices that support access to their consoles.
`drac.default`	DRAC type devices.
`ilo.default`	iLO type devices.
`rsa.default`	Some RSA II type devices.
`rsa.limited.default`	RSA II type devices that support only power commands through their command line interface.
`no template`	• IPMI type devices. • Any type device for which only Native IP access is being configured.

Also see "Command Templates" on page 321.

Configuring Regular Users —Wizard

Figure 3-16 shows the screen that appears when the “Add a regular user” option is selected from the Wizard menu.

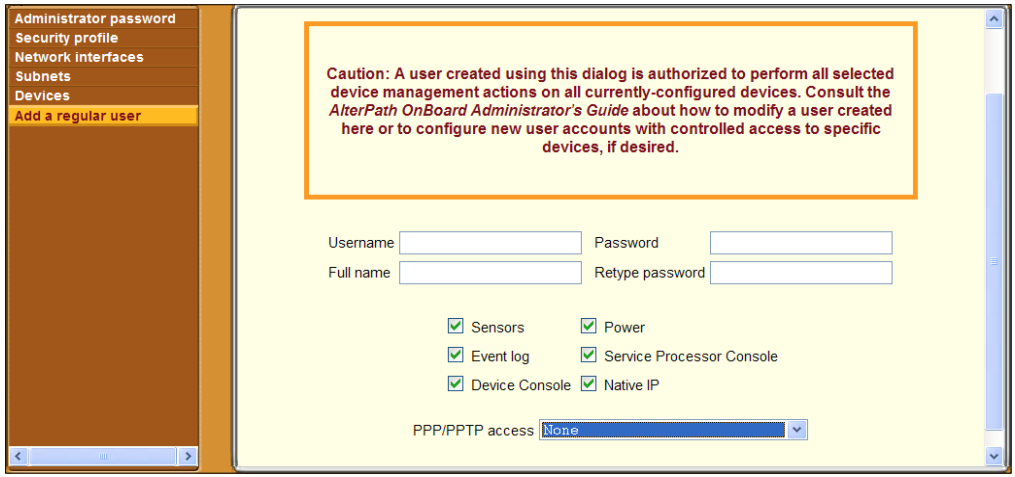


Figure 3-22: “Add a Regular User” Screen—Wizard

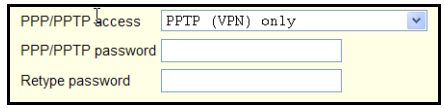
Caution! The Caution at the top of the screen shown in Figure 3-22 is a reminder that the user added using this dialog and adding device management actions for the user gives the user the same device management authorizations on all configured devices. For example, giving the user the “Native IP” authorization on this screen gives the user native IP access to all configured devices. To configure a user account to have more or fewer device management authorizations on one device than on another, the administrative user can use the Config → Users and Groups Screen” to configure specific management authorizations for specific devices.

Table 3-7 describes the parameters that can be set on the screens that appear when the “Add a regular user” option is selected.

Table 3-7: User Configuration Settings

Settings	Notes
Username	Login name required for the user account.

Table 3-7: User Configuration Settings (Continued)

Settings		Notes
Full name		Administratively-defined name to identify the user.
Password		Password used for accessing the OnBoard.
Retype Password		As stated.
• Sensors • Event log • Device Console	• Power • Service Processor Console • Native IP	Check any of the checkboxes to allow the user to perform the selected device management actions
PPP/PPTP access	• None • PPP (dialup only) • PPTP (VPN only) • PPP (dialup) and PPTP (VPN)	Selecting PPP or PPTP for the user causes the two additional fields to display for setting the PPP or PPTP password, as shown in the following screen example: 

▼ *To Create and Authorize a User for Device Management—Wizard*

1. Log into the Web Manager as an administrative user.

   See “To Log Into the Web Manager” on page 75, if needed.
2. Click the “Wizard” button.
3. Click the “Add a regular user” option in the left menu bar.
4. Enter a name in the “Username” field.
5. Enter identifying (GECOS-type) information in the “Full name” field.
6. Enter a password in the “Password” field.
7. Enter the password again in the “Retype password” field.

8. To authorize the user for device management actions on all configured devices, check or leave unchecked the checkboxes next to the name of every allowed action.
9. Select one of the options from the PPP/PPTP access menu.

   With any option other than “None” selected, additional fields appear for entering the PPP or PPTP password.
10. If you selected any option other than “None,” do the following steps.
    a. Enter a password in the “PPP/PPTP password” field.
    b. Retype the password in the “Retype password” field.
11. Click “Save and apply changes.”
12. Click the “Next” button, to go to the Confirm Changes” screen.
13. Click Next to save all changes made in the Wizard and to return to the Web Manager.

Chapter 4
Web Manager “Access” Menu Options

This chapter describes the menu options available to administrative users under the “Access” top menu option.

For an overview of all the Web Manager features and menu options that are available for administrative users, see Chapter 2, “Web Manager Introduction,” if needed.

This chapter covers the topics in the following sections.

“Access” Options Only for Administrative Users	Page 112
Accessing the OnBoard Console	Page 113
Viewing IPDU Status and Managing IPDUs	Page 116
Upgrading AlterPath PM IPDU Software	Page 117

This chapter provides the procedures listed in the following table.

To Download AlterPath PM IPDU Software From Cyclades	Page 119
To Upgrade Software on a Connected IPDU	Page 122

“Access” Options Only for Administrative Users

When the administrative user clicks the “Access” option in the top menu of the Web Manager, four options appear in the left menu, as shown in the following figure.

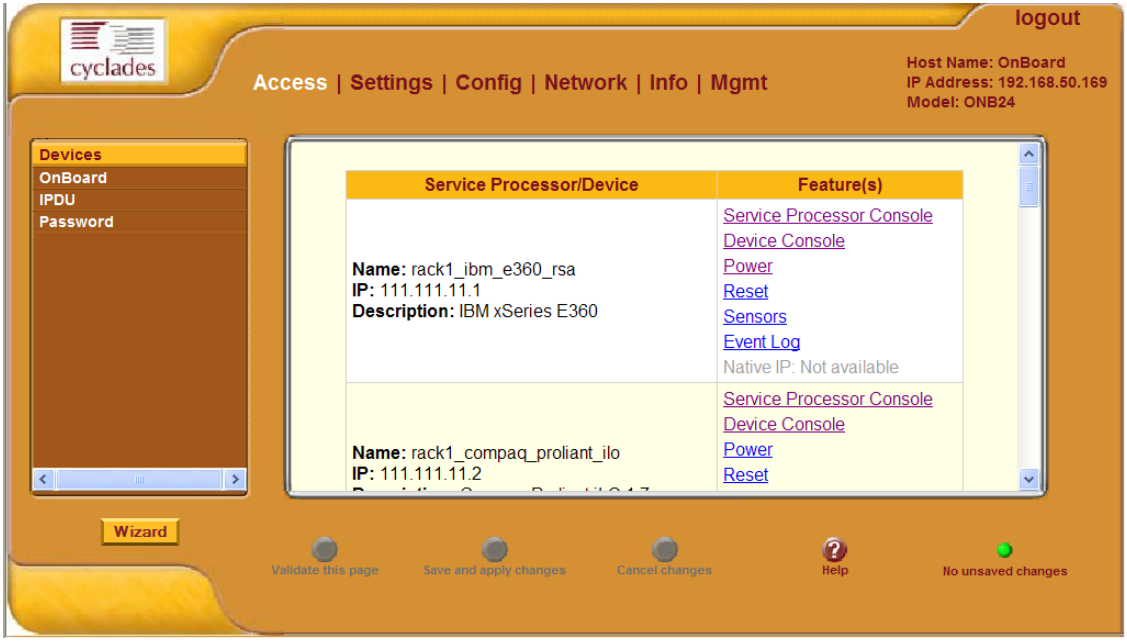


Figure 4-1: Access Menu Options

The menu options that are available when the “Access” option is highlighted in the top menu for administrative users are the same options that are available to regular users, except that administrative users can do additional configuration on some of the screens that are under the IPDU option. See the *AlterPath OnBoard User’s Guide* for information about the following options available to all types of users, which appear for the administrative user under “Access”:

- Devices
- OnBoard
- Password

For the tasks only the administrative user can do under “Access,” see the following sections:

- “Accessing the OnBoard Console” on page 113
- “Viewing IPDU Status and Managing IPDUs” on page 116
- “Upgrading AlterPath PM IPDU Software” on page 117

Accessing the OnBoard Console

When an administrative user clicks the “OnBoard” option under “Access,” a MindTerm window appears with an encrypted SSH connection between the user’s computer and the console. The following figure shows an example.

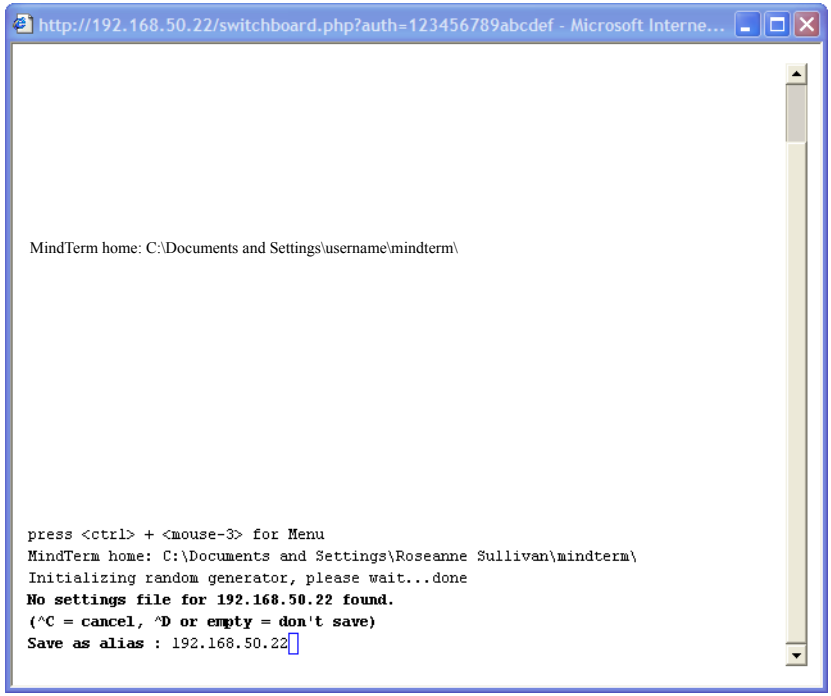


Figure 4-2: Administrative User Console Session Window—Initial Connection from an IP Address

The first time the administrative user accesses the console, the MindTerm prompt shown in Figure 4-2 appears, asking if the IP address of the OnBoard should be saved as an alias in the user’s home directory on the remote

computer. Pressing “Enter” at the prompt brings up the dialog shown in the following screen example.

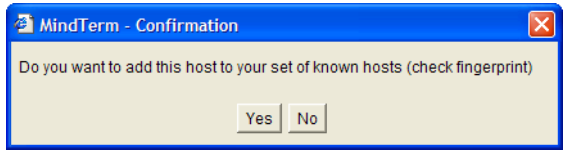


Figure 4-3: OnBoard Console Login Dialog

Clicking “Yes” brings up the login prompt for the OnBoard console, as shown in the following screen example.

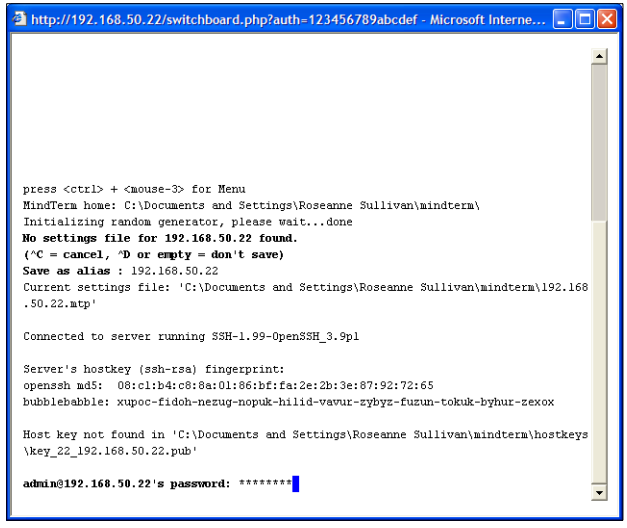


Figure 4-4: OnBoard Console Login Prompt for Administrative Users

After an administrative user enters the correct password and is authenticated, then the administrative user can access the `cycli` utility to perform command line configuration, run the `onbdshell` utility to access devices, and run other commands that do not require root to succeed.

▼ *To Access the OnBoard's Console*

1. Bring up the Web Manager and log in as an administrative user.
2. Go to Access → OnBoard.
   - If this is the first time you accessed the console, MindTerm prompts you to ask if the IP address of the OnBoard should be saved as an alias in your home directory on your workstation. Go to Step 3.
   - If this is not the first time you accessed the console, the login prompt for the OnBoard appears. Go to Step 4.
3. If this is the first time you are accessing the OnBoard's console, do the following steps.
   a. Press "Enter" at the prompt to confirm the saving of the OnBoard's IP address.

      A dialog asks if you want to add the OnBoard to your set of known hosts.

   b. Press the "Yes" button.

      The login prompt for the OnBoard appears.
4. Log into the OnBoard.
5. As desired, do any of the following:
   - Run the `cycli` utility to perform command line configuration.
   - Run the `onbdshell` utility to access devices.
   - Run other commands that do not require root to succeed.

Viewing IPDU Status and Managing IPDUs

The following figure shows the screen that appears when administrative users click the Outlets Manager tab under Access → IPDU.

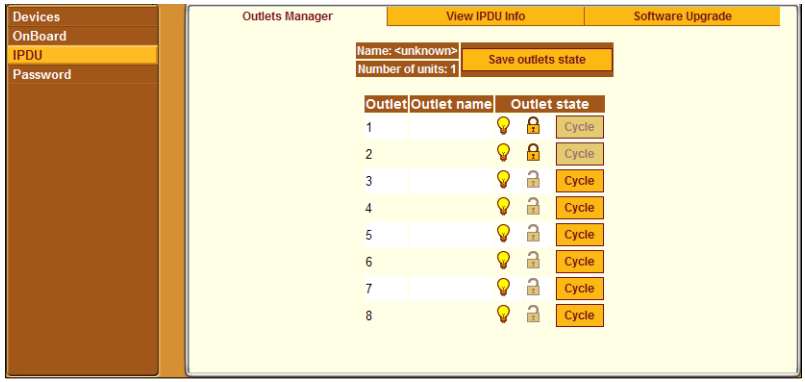


Figure 4-5: Tabs Under Access → IPDU

When administrative users to go Access → IPDU, the following three tabs appear, as shown in the previous figure.

- Outlets Manager
- View IPDU Info
- Software Upgrade

Access to the first two tabs listed above is the same for administrative and authorized users; how to use the first two tabs is described in the *AlterPath OnBoard User's Guide* under the following headings:

- "Managing IPDU Power"
- "Viewing IPDU Information"

For how administrative users can use the Outlets Manager tab to upgrade software on any connected AlterPath PM IPDUs, see "Upgrading AlterPath PM IPDU Software" on page 117.

Upgrading AlterPath PM IPDU Software

The following figure shows the screen layout that appears when an administrative user clicks the Software Upgrade tab under Access → IPDU.

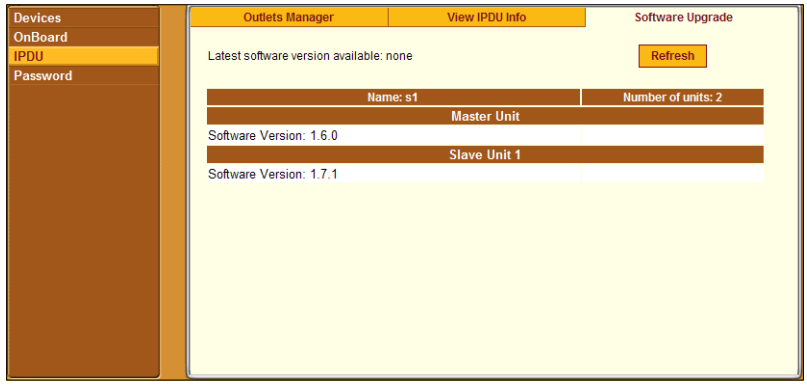


Figure 4-6: IPDU "Software Upgrade" Screen

The table in the screen shown in Figure 4-6 displays information about a directly-connected AlterPath PM IPDU, which is called the "Master Unit," and about any daisy-chained IPDUs, which are named "Slave 1" through "Slave *N*." Each entry displays the version number of the software that is currently installed on the IPDU. The "Refresh" button also appears on the screen.

Figure 4-6 shows entries for a Master Unit, which has software version 1.6.0 and a Slave Unit 1 which has software version 1.7.1.

Note: Daisy-chaining only works if all daisy-chained IPDUs are running the same version of the PM software. The OnBoard administrator must ensure that all connected AlterPath PM IPDUs have the most recent version of the PM software.

Clicking "Refresh" has effects shown in Figure 4-7, but only if both the following are true:

- A `/tmp/pmfirmware` file exists on the OnBoard
- The file contains a more recent version of the PM software than the one currently installed:

As shown in Figure 4-7, the following appear on the screen if the two prerequisites in the previous list are true:

- The “Latest software version available” value changes to match the version in `/tmp/pmfirmware`.
- An “Upgrade” button appears.

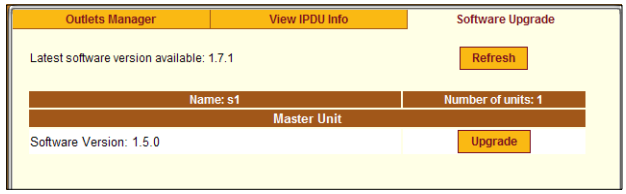


Figure 4-7: Upgrade Button on the IPDU “Software Upgrade” Screen

Pressing the “Upgrade” button starts the upgrade process. The top of the screen shown in the following figure shows the message that displays when the selected AlterPath PM IPDU is being upgraded, and the remaining text in the screen displays when upgrading is complete.

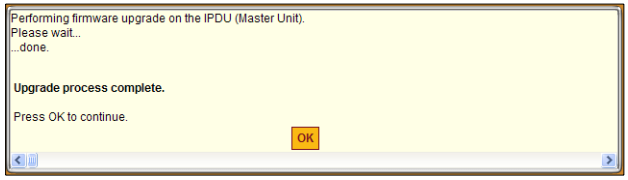


Figure 4-8: IPDU Software Upgrade Dialog

Pressing OK on the dialog shown in Figure 4-8 brings up the “Software Upgrade” screen, which displays the new software version for the selected IPDU.

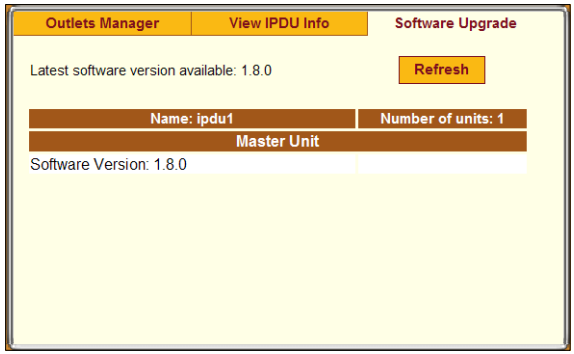


Figure 4-9: IPDU "Software Upgrade" Screen With Upgraded Software

The following table lists the tasks for upgrading software on a connected AlterPath PM IPDU and where they are documented

Table 4-1: Tasks for Upgrading Software on a Connected IPDU

Task	Where Documented
Download an updated version of the AlterPath PM software from Cyclades and install the software in the `/tmp/firmware` directory,	"To Download AlterPath PM IPDU Software From Cyclades" on page 119
Upgrade connected AlterPath PM IPDUs	"To Upgrade Software on a Connected IPDU" on page 122

▼ *To Download AlterPath PM IPDU Software From Cyclades*

An administrative user can use this procedure to download AlterPath PM software from the Cyclades ftp server.

Note: Updated versions of related documents can also be found on the Cyclades website under Support Downloads/Documentation.

After downloading the software onto the OnBoard by following this procedure, the administrative user needs to perform the procedure under "To

Upgrade Software on a Connected IPDU" on page 122 to update the software on connected AlterPath PM IPDU(s).

1. Log into the OnBoard's console as an administrative user.
2. Change to the /tmp directory into which the software needs to be downloaded.

```
[admin@OnBoard admin]# cd /tmp
```

3. Enter the ftp command to access ftp.cyclades.com.

```
[admin@OnBoard tmp]# ftp ftp.cyclades.com
Connected to ftp.cyclades.com (64.186.161.16).
220 "Welcome to Cyclades FTP service."
Name (ftp.cyclades.com:root):
```

4. Enter "anonymous" when prompted for the "Name" and press "Enter" when prompted for the password.

```
Name (ftp.cyclades.com:admin): anonymous
331 Please specify the password.
Password: <Enter>
ftp>
```

5. Change directories to `/pub/cyclades/alterpath/pm/released` and list the directories it contains.

```
ftp> cd /pub/cyclades/alterpath/pm/released
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    2 1006     100          4096 Sep 06  2003 V_1.1.0
drwxr-xr-x    2 1006     100          4096 Feb 23  2004 V_1.2.1
drwxr-xr-x    2 1006     100          4096 Mar 04  2004 V_1.2.2
drwxr-xr-x    2 1006     100          4096 Apr 07  2004 V_1.3.0
drwxr-xr-x    2 1006     100          4096 Nov 18  2004 V_1.4.0
drwxr-xr-x    2 1006     100          4096 Mar 10  2005 V_1.5.0
drwxr-xr-x    3 1006     100          4096 Aug 22 19:03 V_1.6.0
drwxr-xr-x    3 1006     100          4096 Sep 19 20:21 V_1.7.0
drwxr-xr-x    3 1006     100          4096 Nov 02 01:14 V_1.7.1
drwxr-xr-x    3 1006     100          4096 Nov 02 01:14 V_1.8.0
226 Directory send OK.
ftp>
```

As shown in the previous screen example, the directories are named for the software release numbers. The latest version in the example is `V_1.8.0`. If the latest version at the Cyclades site is more recent that the version installed on the IPDU, continue with this procedure to download the latest version.

6. Change directories to the directory with the highest (latest) version number.

```
ftp> cd V_1.8.0
226 Directory send OK.
ftp> ls
150 Here comes the directory listing.
-rw-r--r--    1 1006     100         56916 Nov 02 01:08 PM_180.BIN
-rw-r--r--    1 1006     100            45 Nov 02 01:14 PM_180.BIN.md5sum
drwxr-xr-x    2 1006     100          4096 Nov 02 01:14 doc
-rw-r--r--    1 1006     100          8445 Nov 02 01:08 pmrelease.html
226 Directory send OK.
ftp>
```

As shown in the previous screen example, the directory contains a binary file (PM_*version_number*.BIN) for the latest software version, a checksum file (PM_*version_number*.md5sum), and a doc directory, which contains PDFs of the latest AlterPath PM documentation.

7. Use the get command to get the binary file (for example: PM_180.BIN) and enter pmfirmware as the destination filename

```
ftp> get PM_180.BIN pmfirmware
local: pmfirmware remote: PM_180.BIN
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for PM_180.BIN (56916
bytes).
226 File send OK.
56916 bytes received in 0.01 secs (7783.5 kB/s)
```

8. After the download completes, end the ftp connection, and verify the presence of the pmfirmware file in the /tmp directory.

```
ftp> bye
221 Goodbye.
[admin@OnBoard tmp]$ ls
deb.log             pmfirmware
deb.log.old         wmi
```

9. Log out from the console session and got to "To Upgrade Software on a Connected IPDU."

▼ *To Upgrade Software on a Connected IPDU*

Perform this procedure to upgrade the software on all connected AlterPath PM IPDUs.

This procedure requires the following:

- A more-recent version of the AlterPath PM software than the one shown on the "Software Upgrade" form on the OnBoard must be available from Cyclades, Corp.
- The more-recent version of the AlterPath PM software has been downloaded and copied into the OnBoard's /tmp directory with the

filename `pmfirmware`. For the procedure, see “To Download AlterPath PM IPDU Software From Cyclades” on page 119.

1. Bring up the Web Manager and log in as an administrative user.
2. Go to Access → IPDU → Software Upgrade.

   The Software Upgrade screen displays.
3. Click the “Refresh” button.

   If a `/tmp/pmfirmware` file exists containing a more recent version of the PM software than the one currently installed, the following changes occur on the screen:

   - The value next to “Latest software version available:” changes to match the version in `/tmp/pmfirmware.`
   - An “Upgrade” button appears.
4. Click “Upgrade.”

   A dialog displays while the software is being upgraded.
5. When the OK button displays on the dialog, click OK.
6. Repeat Step 4 and Step 5 for all listed IPDUs until all are upgraded to the same level.

Chapter 5
Web Manager “Settings” Menu Options

This chapter describes the menu options available to administrative users under the “Settings” top menu option.

For an overview of the Web Manager features that are available only for administrative users and for how to use the configuration wizard, see Chapter 2, “Web Manager Introduction,” if desired.

This chapter covers the topics listed the following table.

Options Under “Settings”	Page 126
Configuring the AUX Port for Modem or Power Management	Page 127
Configuring the AUX Port for IPDU Power Management	Page 128
Configuring IPDU Power Management	Page 132
Configuring PCMCIA Cards	Page 139
Configuring System Date and Time	Page 150
Configuring the Boot File Location	Page 152
Configuring an Alternate Help File Location	Page 156

This chapter provides the procedures listed in the following table.

To Configure an AUX Port for IPDU Power Management	Page 128
To Configure an AUX Port for Modem Access	Page 131
To Enable Overcurrent Protection for an AlterPath PM IPDU	Page 135
To Configure a User to Manage Power Outlets on a Connected IPDU	Page 137
To Configure an Alias and a Power Up Interval for an IPDU Outlet	Page 138
To Begin Configuring a PCMCIA Card	Page 142

To Configure a Modem PCMCIA Card	Page 145
To Configure a Compact Flash PCMCIA Card	Page 149
To Configure System Date and Time	Page 151
To Configure OnBoard Boot	Page 155
To Specify a New Location for OnBoard Help Files	Page 157

Options Under “Settings”

When an administrative user clicks the “Settings” option in the top menu of the Web Manager, five options appear in the left menu, as shown in the following figure.

Figure 5-1: “Settings” Menu Options

The following table lists the options that appear when an administrative user clicks “Settings” and provides links to where the options are described.

Table 5-1: Options Under Settings

Option	Where Described
AUX port	“Configuring the AUX Port for Modem or Power Management” on page 127.
IPDU	“Configuring IPDU Power Management” on page 132

Table 5-1: Options Under Settings (Continued)

Option	Where Described
PCMCIA	“Configuring PCMCIA Cards” on page 139
Date/time	“Configuring System Date and Time” on page 150
Boot configuration	“Configuring the Boot File Location” on page 152
Help	“Configuring an Alternate Help File Location” on page 156

Configuring the AUX Port for Modem or Power Management

When an administrative user clicks the “AUX port” option under “Settings,” a screen like the one shown in the following figure appears.

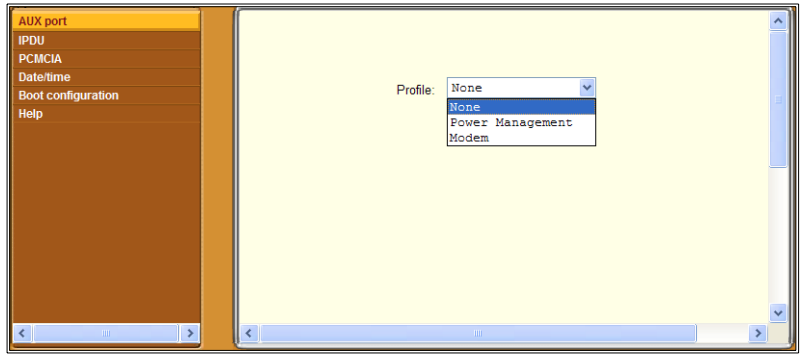


Figure 5-2: Settings → Aux Port Screen

The administrative user can use the Settings → AUX port screen to configure either of the following types of optional devices, if they are connected to the AUX port:

- One or more AlterPath PM IPDUs
- An external modem

For how to connect IPDUs and external modems, see the “Advanced Procedures” chapter in the *AlterPath OnBoard Installation Guide*.

Configuring the AUX Port for IPDU Power Management

The following figure shows the screen that appears when the administrative user selects the Power Management option from the “Profile” menu on the Settings → AUX port screen.

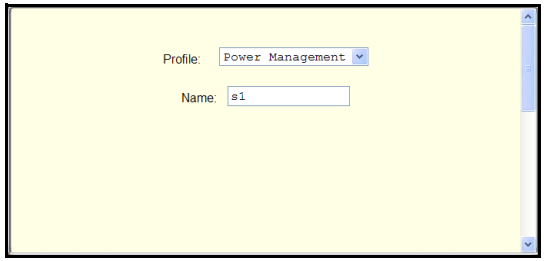


Figure 5-3: Settings → AUX Port → Power Management

▼ To Configure an AUX Port for IPDU Power Management

This procedure assumes that an AlterPath PM IPDU is connected to the AUX port of the OnBoard.

1. Log into the Web Manager as an administrative user.
2. Go to Settings → AUX Port.
3. Make sure the “Power Management” option is selected from the “Profile” menu.
4. Optional: Enter a name for the connected AlterPath PM IPDU in the “Name” field.
5. Click “Save and apply changes.”

Configuring the AUX Port for a Modem

The following figure shows the screen that appears when the administrative user selects the Modem option from the “Profile” menu on the Settings → AUX port screen.

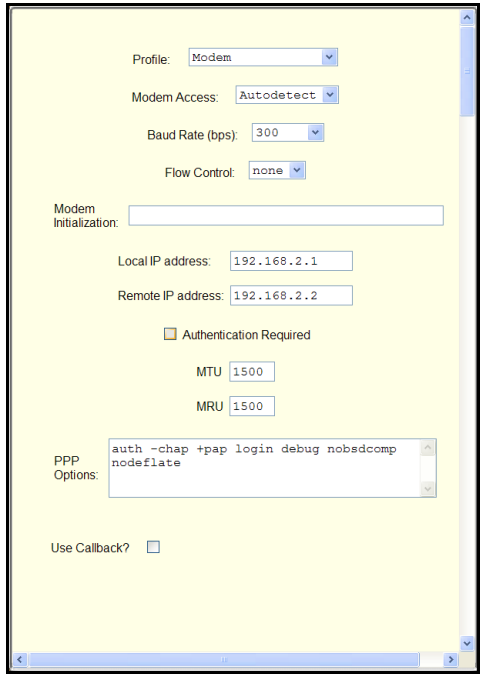


Figure 5-4: Settings → AUX Port → Modem

See Table 1-20 on page 44 for descriptions of the valid values to be entered on the modem configuration screen.

Figure 5-4 shows the fields and pull-down menus that appear when “Autodetect” is selected from the “Modem Access” pull-down menu. Because autodetection can detect either a PPP or Login access attempt, the screen has fields and pull-down menus for configuring all the parameters that apply to both options.

Figure 5-5 shows the fields and pull-down menus that appear when the PPP option is selected from the “Modem Access” pull-down menu.

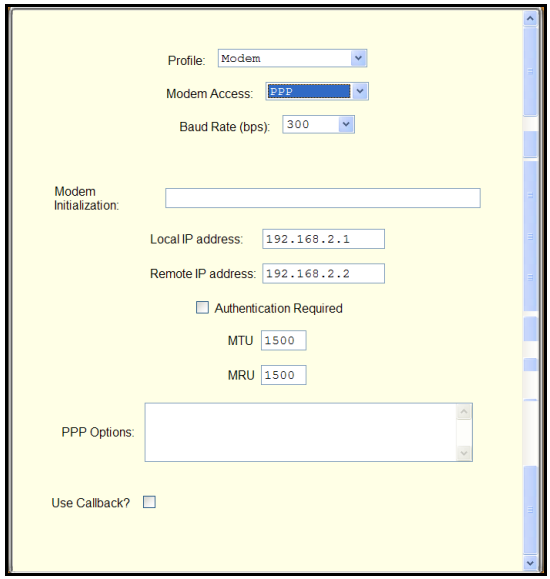


Figure 5-5: Settings → AUX Port → Modem

When the "Use Callback?" checkbox is checked, the "Callback Number" field appears, as shown in the following figure.

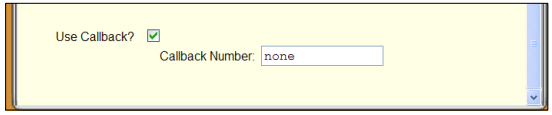


Figure 5-6: Callback Number Field Under Settings → AUX Port → Modem

When the "Login" option is selected from the "Modem Access" pull-down menu, the fields shown in the following figure appear.

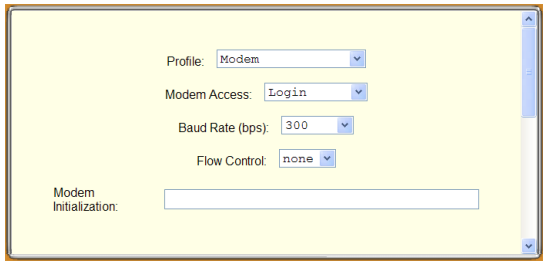


Figure 5-7: Settings → AUX Port → Modem

▼ *To Configure an AUX Port for Modem Access*

This procedure assumes that an external modem is connected to the AUX port of the OnBoard. The values to select or to enter for modem configuration are described in Table 1-20 on page 44.

1. Log into the Web Manager as an administrative user.
2. Go to Settings → AUX Port.
3. Make sure the “Modem” option is selected from the “Profile” menu.
4. Choose Autodetect, Login, or PPP from the “Modem access” menu.
5. Select a baud rate from the “Baud Rate” pull-down menu.
6. If you chose Autodetect or Login, select an option from the “Flow Control” menu.
7. Enter a modem chat string in the “Modem Initialization” field.
8. If you chose PPP or Autodetect, do the following:
   a. Enter a IP address or accept the default provided in the “Local IP address” field.
   b. Enter a IP address or accept the default provided in the “Remote IP address” field.
   c. Enable or disable authentication by checking or leaving unchecked the “Authenticating Required” checkbox.
   d. Accept or change the value in the MTU field.
   e. Accept or change the value in the MRU field.

f. Accept or change PPP options as desired in the “PPP Options” field.

g. Enable or disable callback by checking or leaving unchecked the “Use Callback?” checkbox.

h. If you enabled callback, enter a callback phone number in the “Callback Number” field.

9. Click “Save and apply changes.”

Configuring IPDU Power Management

When an administrative user clicks the “IPDU” option under “Settings,” a screen like the one shown in the following figure appears.

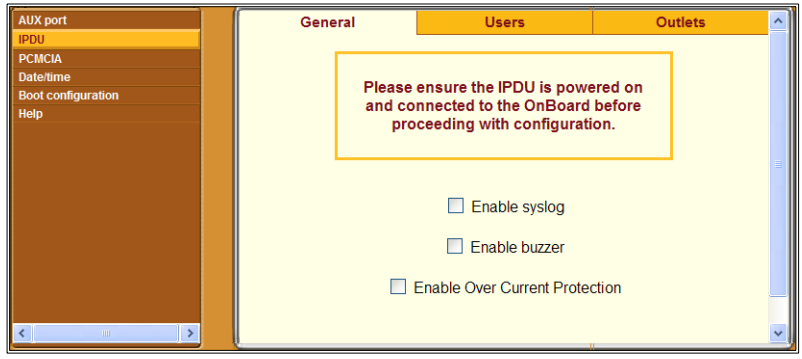


Figure 5-8: Settings → IPDU Screen

As shown in Figure 5-8, when the AUX port is configured for power management, three tabs appear for configuring one or more connected IPDU(s).

Selecting Settings → IPDU without first configuring the AUX port for power management displays the message shown in the following figure.

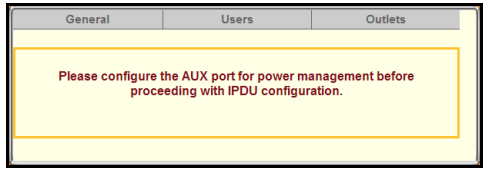


Figure 5-9: Settings → IPDU Screen Without AUX Port Configuration

Note: The first IPDU connected to the AUX port is called the Master Unit. An additional IPDU that is daisy-chained to the first IPDU is called a "Slave Unit."

The following table lists the tabs on the Settings → IPDU screen with links to the sections where they are described.

Table 5-2: Options Under Settings → IPDU

Option	Where Described
General	"Configuring Over Current Protection for an IPDU" on page 133.
Users	"Configuring Users to Manage Power Outlets on a Connected IPDU" on page 135.
Outlets	"Configuring Names and Power Up Intervals for Outlets on a Connected IPDU" on page 137

Configuring Over Current Protection for an IPDU

The Settings" → IPDU → General tab displays a warning and three options with checkboxes, as shown in the following screen example

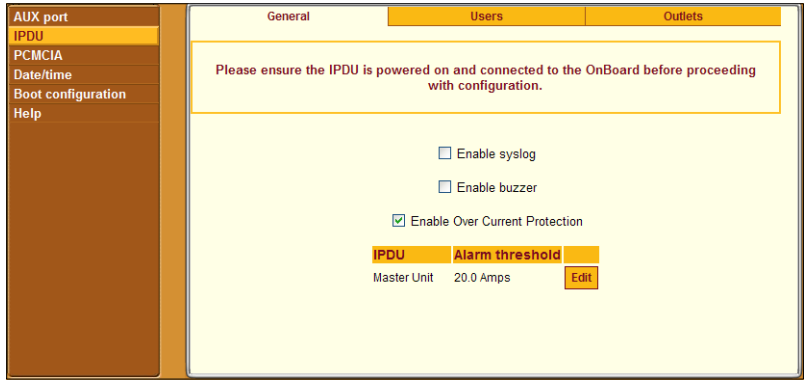


Figure 5-10: Settings IPDU General Screen

The settings on the page shown in Figure 5-8 apply to all AlterPath PM IPDUs that are either directly-connected or daisy-chained to the AUX port:

- "Checking "Enable Over Current Protection" allows an administrative user to specify a maximum number of Amps. When the maximum number of Amps is exceeded (and, therefore, an "overcurrent" state exists), the OnBoard generates an alarm. The type of alarm depends on whether "Enable syslog" or "Enable buzzer" or both are checked.
- Checking "Enable syslog" causes syslog messages to be sent to the console if the maximum current is exceeded.
- Checking "Enable buzzer" causes a buzzer to sound on the AlterPath PM if the maximum current is exceeded.

Checking the "Enable Over Current Protection" checkbox brings up the table like the one in the following screen example. The example shows entries for a Master and a Slave Unit, with Alarm Threshold values already configured by an administrative user.

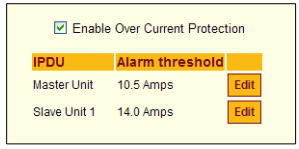


Figure 5-11: Settings IPDU General Screen

Clicking the Edit button in the entry for an IPDU brings up the screen shown in the following screen example.

Figure 5-12: Edit Alarm Threshold for IPDU Dialog

The appropriate value to enter in the “Alarm Threshold” field varies from one AlterPath PM to the other. The value can be entered either as a number or as a number with a decimal point, for example, 10 amps or 14.5 amps.

▼ *To Enable Overcurrent Protection for an AlterPath PM IPDU*

1. Log into the Web Manager as an administrative user.
2. Go to Settings → IPDU → General.
3. Check “Enable Over Current Protection,” then do the following steps.
   a. Click the “Edit” button next to the IPDU on which you want to set alarm threshold.

      The “Edit Alarm Threshold for IPDU Dialog” appears.

   b. Enter the appropriate number of Amps for the selected type of AlterPath PM in the “Alarm Threshold” field.
   c. Click OK.
4. Check “Enable syslog” to enable messages to be sent to the console if the alarm threshold is exceeded.
5. Check “Enable buzzer” to cause a buzzer to sound on the PM if the alarm threshold is exceeded.
6. Click OK.
7. Click “Save and apply changes.”

Configuring Users to Manage Power Outlets on a Connected IPDU

On the Users screen under Settings → IPDU, an administrative user can authorize regular users to manage power outlets. The following figure shows the screen that displays when a single AlterPath PM is connected to the AUX port, which has been configured for power management. The list is empty because no users have yet been configured for power management.

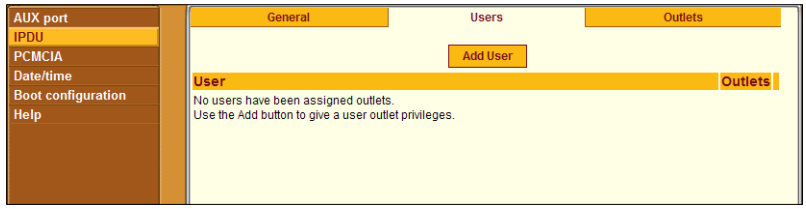


Figure 5-13: Settings → IPDU → Users Screen

Clicking "Add" brings up the dialog shown in the following figure, where an administrative user can specify one or more comma-separated user names and one or more outlets.

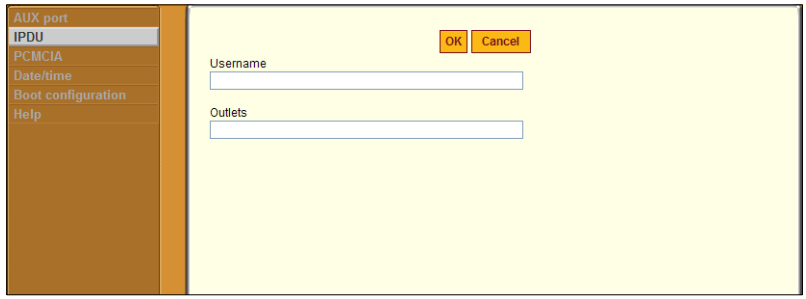


Figure 5-14: Settings → IPDU → Users → Add User Dialog

A comma can be used to separate outlet numbers, and a hyphen can be used to indicate a range of outlets (for example: 1, 3, 5, 6-8).

After a user is added and the OK button is clicked, the user's name is added to the list on the Users Manager form along with the numbers of the outlets the user is authorized to manage, as shown in the following figure.

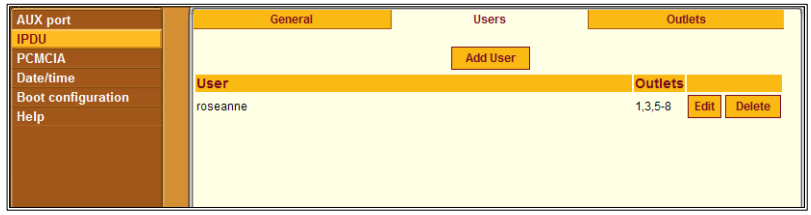


Figure 5-15: Settings → IPDU → Users With a User Added

▼ To Configure a User to Manage Power Outlets on a Connected IPDU

This procedure assumes the following prerequisites:

- An AlterPath PM IPDU is connected to the AUX port of the OnBoard.
- The AUX port is configured for power management (as described in "To Configure an AUX Port for IPDU Power Management" on page 128).
- The user account has been defined under "To Create and Authorize a User for Device Management" on page 174.

1. Log into the Web Manager as an administrative user.
2. Go to Settings → IPDU → Users.
3. Click the "Add User" button.
4. Enter the name of a user in the "Username" field.
5. Enter the outlets to manage in the "Outlets" field.
6. Click OK.
7. Click "Save and apply changes."

Configuring Names and Power Up Intervals for Outlets on a Connected IPDU

On the Outlets screen under Settings → IPDU, an administrative user can assign a name to a power outlet and change the number of seconds that must elapse between when the selected outlet is turned on and another outlet can be turned on.

The following figure shows the default screen. The Name column is empty because no names have been configured for any outlets. The default power up interval of 0.5 seconds displays in the "Interval" column if an administrator has not previously changed any of the intervals.

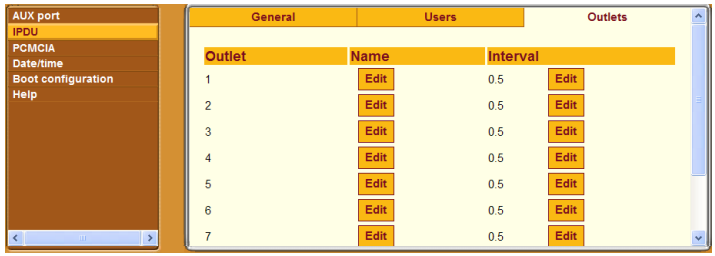


Figure 5-16: Settings → IPDU → Outlets Screen

When the "Edit" button is clicked in the "Name" column, the outlet name dialog box appears with the field shown in the following figure.

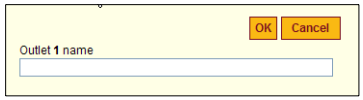


Figure 5-17: Outlet Name Dialog

When the "Edit" button is clicked in the "Interval" column, the outlet power up interval dialog box appears with the field shown in the following figure.

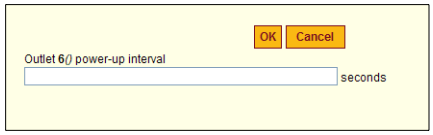


Figure 5-18: Outlet Power Up Interval Dialog

Intervals can be specified using numbers or numbers followed by decimals, such as 10 or 7.5. Clicking OK saves the entries.

▼ *To Configure an Alias and a Power Up Interval for an IPDU Outlet*

1. Log into the Web Manager as an administrative user.
2. Go to Settings → IPDU → Outlets.
3. To assign or change an outlet name, do the following steps.
   a. Click the "Edit" button in the outlet's Name column.

      The outlet name dialog box appears.

b. Enter a name in the "Outlet *N* name" field.

c. Click OK.

4. To assign or change an outlet's power-up interval, do the following steps.

a. Click the "Edit" button in the outlet's Interval column.

The outlet power up interval dialog box appears.

b. Enter a number of seconds in the "Outlet N power-up interval" field.

c. Click OK.

5. Click "Save and apply changes."

Configuring PCMCIA Cards

When an administrative user clicks the PCMCIA option under "Settings," a screen appears like the one shown in the following figure.

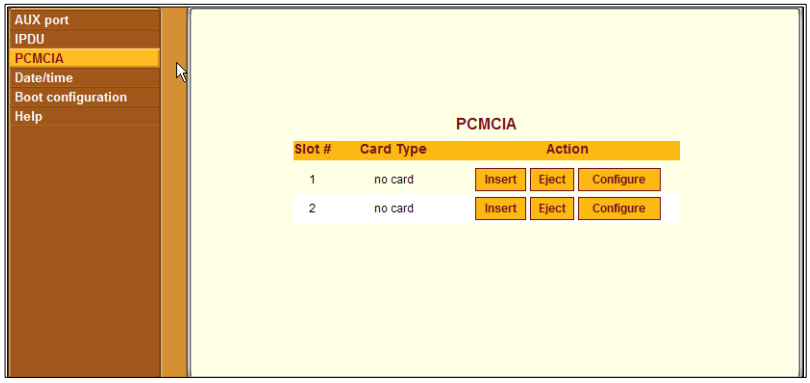


Figure 5-19: Settings → PCMCIA Screen

Figure 5-19 shows the screen's appearance when no card has been inserted or configured in either slot.

An administrative user can use the PCMCIA screen to insert, eject, and configure the following types of cards:

- Modem
- Ethernet (10/100BaseT)
- Compact flash

See the *AlterPath OnBoard Installation Guide* for a list of supported cards. Also check the release notes at the Cyclades website for additions to the list of supported cards.

As shown in Figure 5-19, three buttons appear under the Action column in the PCMCIA table. The following table shows how the buttons are used and provides links to related procedures.

Table 5-3: PCMCIA Action Buttons

Action	Notes	Where Described
Insert	Click this button before physically inserting the card.	"Inserting a PCMCIA Card" on page 140
Eject	Click this button before physically ejecting the card.	"Ejecting a PCMCIA Card" on page 141
Configure	Click this button to bring up a dialog for configuring the card according to its type	"Configuring a PCMCIA Card" on page 142

Inserting a PCMCIA Card

Clicking an "Insert" button on an entry for a PCMCIA card slot brings up a dialog like the one shown in the following figure.

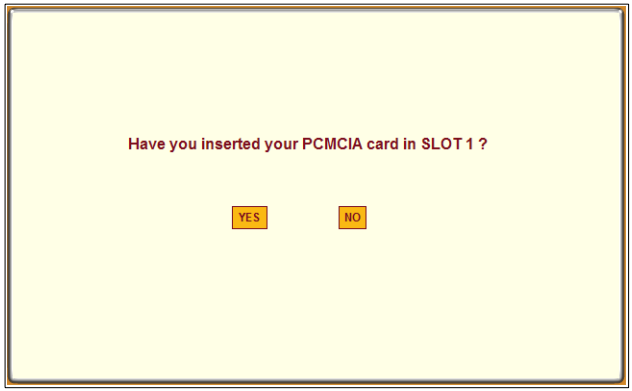


Figure 5-20: Insert PCMCIA Query

After the card is inserted, clicking "YES" in the dialog causes information to appear in the "Card Type" column, as shown in the following figure.

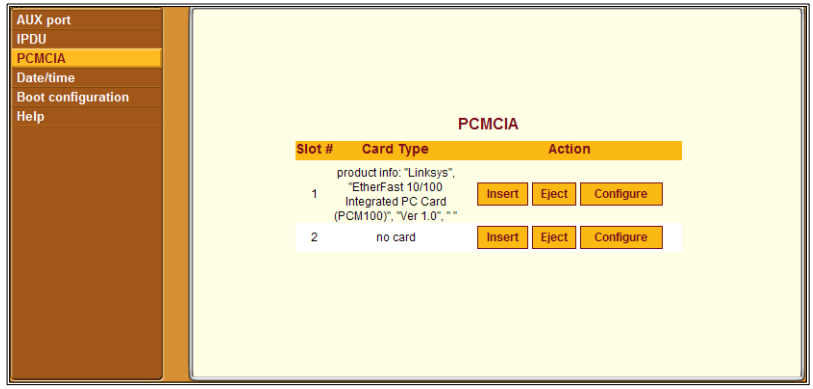


Figure 5-21: Example: PCMCIA Ethernet Card inserted in Slot 1

Ejecting a PCMCIA Card

Clicking an “Eject” button brings up a screen like the one shown in the following figure.

Figure 5-22: Eject PCMCIA Dialog

Clicking OK ejects the card in preparation for physical ejection.

Configuring a PCMCIA Card

The following procedure describes the configuration steps to begin configuring any PCMCIA card and includes links to procedures for configuring specific types of cards.

▼ To Begin Configuring a PCMCIA Card

1. Log into the Web Manager as an administrative user.
2. Go to Settings → PCMCIA.

   The PCMCIA screen appears.
3. Click the "Insert" button on the line for the slot in which you are installing the PCMCIA card.
4. Insert a PCMCIA card into one of the slots on the front of the OnBoard.

   See the "Advanced Procedures" chapter in the *AlterPath OnBoard Installation Guide* for guidance about the order of insertion and other hardware-specific instructions, if needed.
5. Click OK.

   The card type appears under the "Card Type" column.
6. Click the "Configure" button.

   The "PCMCIA card configuration" dialog box for the selected slot appears.
7. Select the desired PCMCIA card type to configure from the pull-down menu.
8. Go to the appropriate section for background information, if needed, or go directly to the related procedure.

Configuring a Modem PCMCIA Card	Page 143
To Configure a Modem PCMCIA Card	Page 145
Configuring an Ethernet PCMCIA Card	Page 146
To Configure an Ethernet PCMCIA Card	Page 147

Configuring a Compact Flash PCMCIA Card	Page 148
To Configure a Compact Flash PCMCIA Card	Page 149

Configuring a Modem PCMCIA Card

When a modem card is inserted into the selected slot, clicking the “Configure” button on the Settings → PCMCIA screen brings up a dialog like the one shown in the following figure.

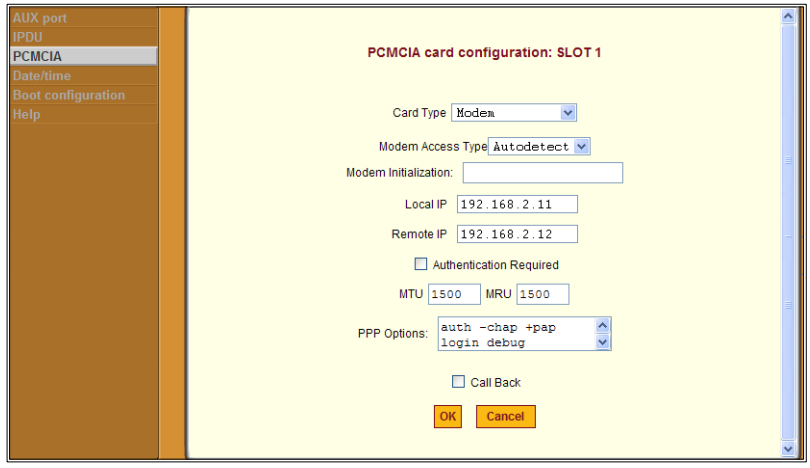


Figure 5-23: Settings → PCMCIA → Configure Modem Dialog

An administrative user can use the Settings → PCMCIA → Configure Modem dialog to enable a remote user to dial into the OnBoard through an installed modem PCMCIA card and to optionally enable callback. The values to select or to enter for modem configuration are described in Table 1-20, “Modem Configuration Field and Menu Definitions,” on page 44.

Note: When Autodetect is selected, all the fields for configuring PPP and Login appear on the same screen and must be filled out, since either type of access (PPP or Login) may be automatically detected.

If the “Call Back” checkbox is selected, then an additional field for the phone number appears, as shown in the following example.

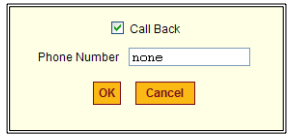


Figure 5-24: Settings → PCMCIA → Configure Modem Callback

If "Login" is selected from the "Modem Access Type" pull-down menu, the following fields and checkbox appear.

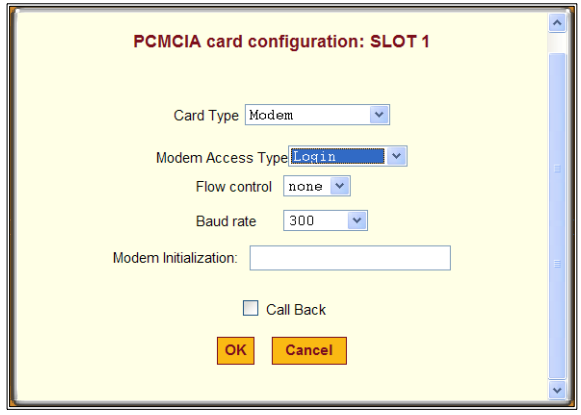


Figure 5-25: Settings → PCMCIA → Configure Modem → Login

If "PPP" is selected from the "Modem Access Type" pull-down menu, the following fields and checkboxes appear.

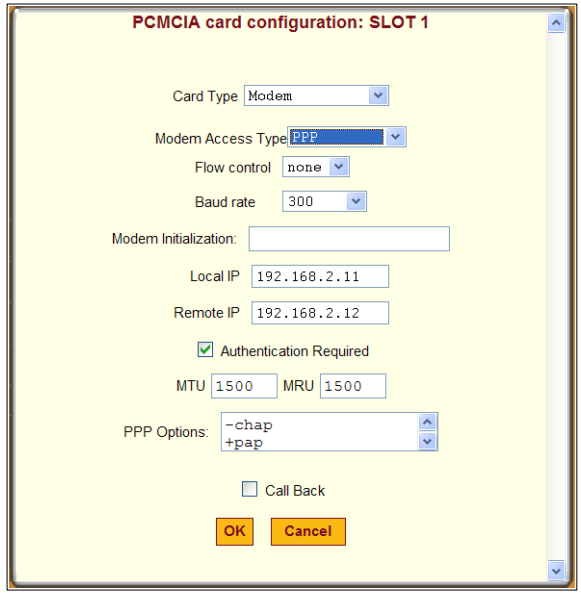


Figure 5-26: Settings → PCMCIA → Configure Modem → PPP

▼ *To Configure a Modem PCMCIA Card*

This procedure assumes that a PCMCIA modem card is inserted into a slot on the OnBoard and the steps under "To Begin Configuring a PCMCIA Card" on page 142 are complete. See Table 1-20, "Modem Configuration Field and Menu Definitions," on page 44 for the values that an administrative user needs to select or to enter for modem configuration, if needed.

1. Make sure that "Modem" is selected from the "Card Type" pull-down menu on the PCMCIA card configuration dialog.
2. Select either "Login," "Autodetect," or "PPP" from the "Modem Access Type" pull-down menu.
3. Enter a modem chat string in the "Modem Initialization" field.
4. To enable callback, do the following steps.
   a. Check the "Call Back" check box.

      The Phone Number field appears on the Slot dialog box.

b. Enter a number for the OnBoard to use when calling back the remote user's modem.

5. If you selected either the "PPP" or "Autodetect" modem access types, do the following steps:

a. Enter a local IP address or accept the default provided in the "Local IP address" field.

By default, the IP address of the OnBoard is used. Only change the local IP address if you have a specific reason to do so.

b. Enter a remote IP address or accept the default provided in the "Remote IP address" field.

Only change the remote IP address if you have a specific reason to do so.

c. Enable or disable authentication during modem access by checking or leaving unchecked the "Authenticating Required" checkbox.

d. Accept or change the value in the MTU field.

e. Accept or change the value in the MRU field.

f. Enter PPP options as desired in the "PPP Options" field.

6. Click OK.

7. Click "Save and apply changes."

Configuring an Ethernet PCMCIA Card

Clicking the "Configure" button on the Settings → PCMCIA screen brings up the dialog shown in the following figure when an Ethernet card is inserted in the selected slot and the DHCP checkbox is checked.

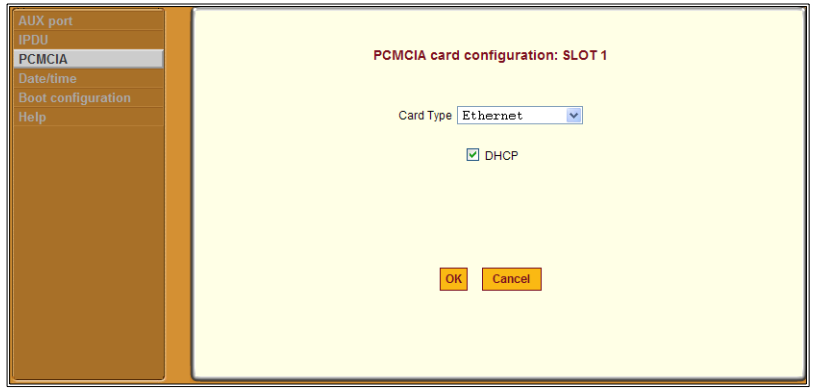


Figure 5-27: Settings → PCMCIA → Configure Ethernet Dialog

As shown in Figure 5-28, the dialog for configuring an Ethernet card displays additional fields for specifying the IP address, network mask, and gateway when the DHCP checkbox is not checked.

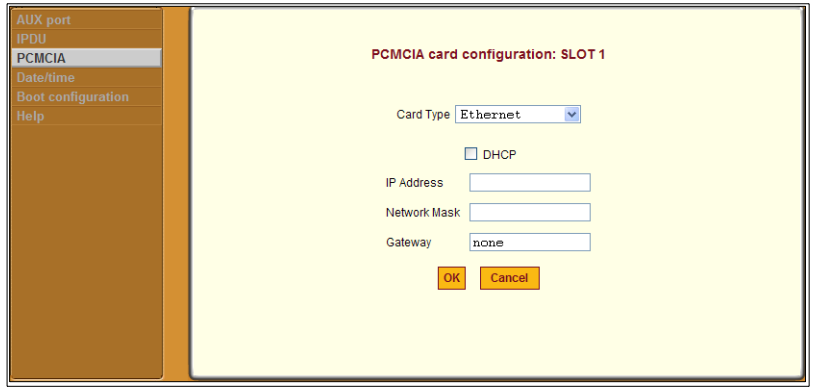


Figure 5-28: Settings → PCMCIA → Configure Ethernet Dialog Without DHCP

▼ *To Configure an Ethernet PCMCIA Card*

This procedure assumes that an Ethernet card is inserted into a PCMCIA slot on the OnBoard and the steps under “To Begin Configuring a PCMCIA Card” on page 142 are complete.

1. Make sure that “Ethernet” is selected from the “Card Type” pull-down menu on the PCMCIA card configuration dialog.

2. To enable DHCP, check the DHCP checkbox, and go to Step 4.
3. To define basic network parameters that enable the use of a static IP address, do the following steps.
   a. Enter an IP address in the “IP Address” field.
   b. Enter a netmask in the “Network Mask” field.
   c. Enter the IP address for a gateway host or enter “none” in the “Gateway” field.
4. Click OK.
5. Click “Save and apply changes.”

Configuring a Compact Flash PCMCIA Card

When a compact flash card is inserted in the selected slot, clicking the “Configure” button on the Settings → PCMCIA screen brings up a dialog like the one shown in the following figure.

Figure 5-30 shows the “Mount Compact Flash Card” checkbox unchecked

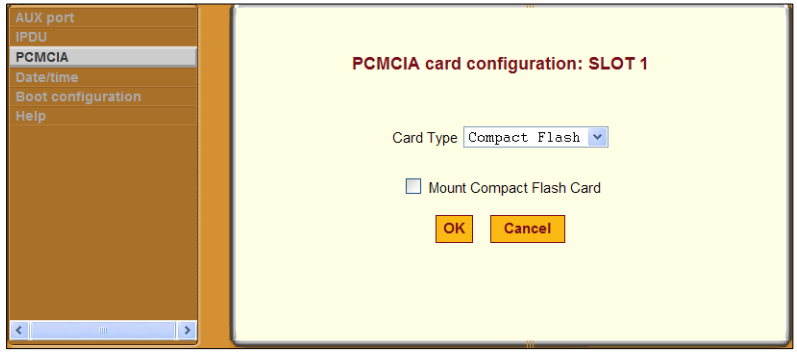


Figure 5-29: Settings → PCMCIA → Configure Compact Flash Dialog: Mount Option Unchecked

Figure 5-30 shows the “Mount Compact Flash Card” checkbox checked, and the “Auto” option selected from the “File System” pull-down menu.

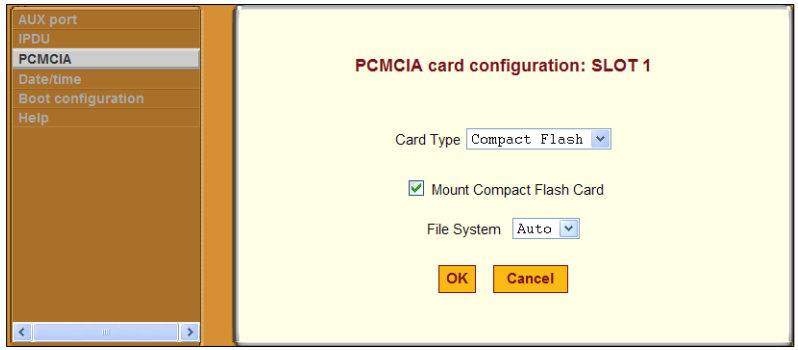


Figure 5-30: Settings → PCMCIA → Configure Compact Flash Dialog

The three options on the “File System” pull-down menu are listed here:

- Auto
- Vfat
- Ext2

▼ *To Configure a Compact Flash PCMCIA Card*

This procedure assumes that a compact flash card is inserted into a PCMCIA slot on the OnBoard and the steps under “To Begin Configuring a PCMCIA Card” on page 142 are complete.

1. Make sure that “Compact Flash” is selected from the “Card Type” pull-down menu on the PCMCIA card configuration dialog.
2. To mount a filesystem from the compact flash memory, click the “Mount Compact Flash Card” checkbox.
3. Select an option from the “File System” menu.
4. Click OK.
5. Click “Save and apply changes.”

Configuring System Date and Time

When an administrative user clicks the Date/time option under Settings, a screen appears like the one shown in the following figure.

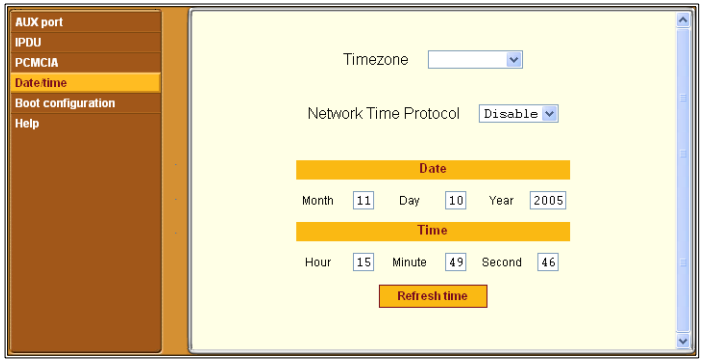


Figure 5-31: Settings → Date/time Screen

An administrative user can use the Settings → Date/time screen for configuring the timezone and for specifying how the OnBoard sets its time and date.

The “Network Time Protocol” pull-down menu provides two options:

- Disable
- Enable,

The “Timezone” pull-down menu lists world timezones based on GMT, as shown in the following figure.

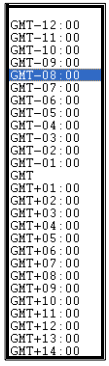


Figure 5-32: Settings → Date/time Screen: Timezone Pull-down

When Enable is selected from the “Network Time Protocol” pull-down menu, the “NTP server IP” field appears. An administrative user needs to specify the IP address of an NTP server in the NTP server field, as shown in Figure 5-33.

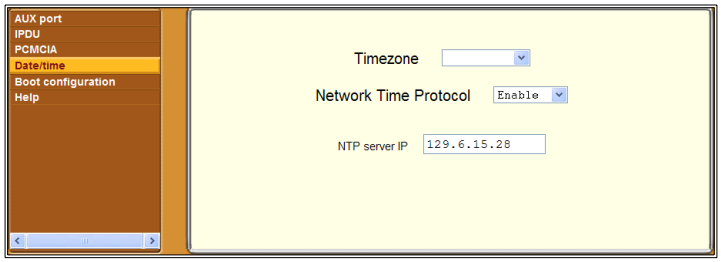


Figure 5-33: Settings → Date/time Screen With NTP Fields

When Disable is selected from the Network Time Protocol menu, Date and Time configuration fields appear, as shown in Figure 5-31, for an administrative user to enter the date and time manually.

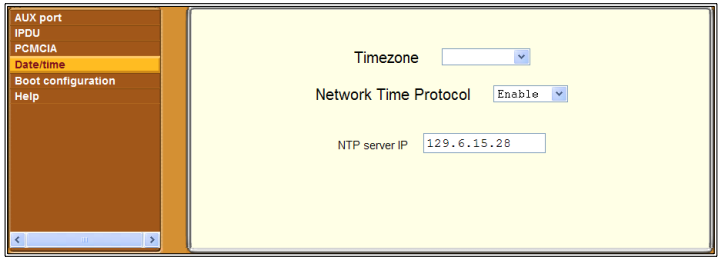


Figure 5-34: Settings → Date/time Screen

▼ *To Configure System Date and Time*

1. Select a timezone from the “Timezone” pull-down menu.
2. To enable the OnBoard to get its time from an NTP server, do the following steps.
   a. Select “Enable” from the Network Time Protocol pull-down menu.
   b. Enter the IP address of the NTP server in the “NTP server IP” field.
3. To manually define the date and time, do the following steps.
   a. Enter the month, day, and year in the “Month,” “Day,” and “Year” fields.

b. Enter the hour, minute, and second in the “Hour,” “Minute,” and “Second” fields.

c. Click the “Refresh time” button.

4. Click OK.

5. Click “Save and apply changes.”

Configuring the Boot File Location

When an administrative user selects the Boot configuration option under Settings, a screen appears like the one shown in the following figure.

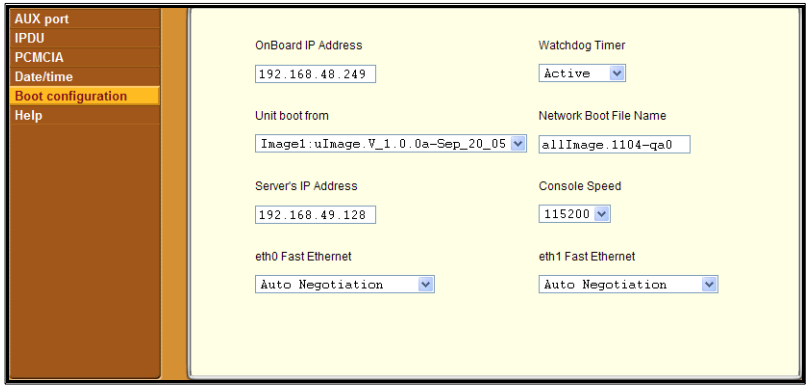


Figure 5-35: Settings → Boot Configuration Screen

An administrative user can use the Settings → Boot configuration screen to redefine the location from which the OnBoard boots. By default, the OnBoard boots from a boot file in the on-board Flash memory. Booting from the resident software is strongly recommended. Network boots should be reserved only for troubleshooting or upgrading. The differences between booting from a local copy of the software image and booting from the network are explained further in the following sections.

Specifying the Boot File Location

The “Unit boot from” pull-down menu lists the “Network” option for booting from a TFTP boot server on the network along with one or two boot images that reside on the OnBoard. Two options appear (“Network” and “Image1”), as shown in the following figure, if only one boot image is found on the OnBoard.

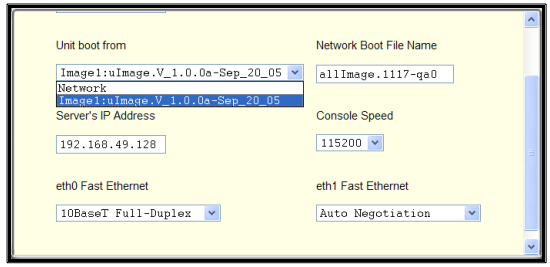


Figure 5-36: Settings → Boot Configuration → Unit Boot Menu

The default image stored on the OnBoard is shown in the example with the name `Image1:uImage.V_1.0.0a-Sep_20_05`. A second image appears in the list only if the software has been upgraded.

Local Boot Options

To understand the local options on the "Unit boot from" menu, you need to understand how the OnBoard handles software upgrades:

- The OnBoard initially boots from a software image referred to as "Image1."
- The first time a new software version is downloaded and installed from Cyclades, the new image is stored as "Image2" in the flash memory and the configuration is changed so the OnBoard boots from "image 2."
- The second time a new software version is downloaded and installed, the latest image is stored as "Image 1," and the OnBoard configuration is changed to boot from "Image1."
- Subsequent downloads are stored following the same pattern, alternating "Image1" with "Image2."

In the "Unit boot from" pull-down menu, the entry for the *current boot* image is selected by default.

After a software upgrade, the boot file location choices are:

- Network
- Image1:*image_filename*
- Image2:*image_filename*

The word “image” is followed by the number, followed by a colon (:), followed by the name of the file, including the version number. The menu item has the following format:

`image1:zvmppconb.v`*`version_number`*

The entry for the first release of the software, which is installed in the image1 area, is:

`image1:zvmppconb.v100`

After one or more software upgrades have been performed, a second image also appears in the menu, for example:

`image1:zvmppconb.v100`

`image2:zvmppconb.v101`

If you want to boot from another image than the one currently selected, you can select that image from the “Unit boot from” menu.

Network Boot Options

Network boots are recommended only for troubleshooting or for possible downloads of new software images that can then be stored in the on-board flash memory, as described in “To Replace a Boot Image From a Network Boot in U-Boot Monitor Mode” on page 379.

To boot from a boot server, you can select “Network” and configure a boot server.

For network boot to work, make sure the following prerequisites are done.

- A TFTP server must be available to the OnBoard on the network.
- An upgraded OnBoard boot image file must be downloaded from Cyclades and must be available on the boot server.
- The OnBoard must have a fixed IP address and you must know the address.

Boot Fields and Menu Options

The fields and menu options for boot configuration are described in the following table.

Table 5-4: Boot Configuration Fields and Options

Field or Value Name	Description
OnBoard IP address	A new IP address for the OnBoard.
Watchdog timer	Whether the watchdog timer is active. Choices are: • InActive • Active If the watchdog timer is active, the OnBoard reboots if the software crashes. See “To Configure OnBoard Boot” on page 155 for how the watchdog timer can be activated or deactivated.
Unit boot from	Choose a local image or “Network” from the list.
Network boot file name	The name of the boot file being accessed over the network.
Server’s IP address	The IP address for the boot server.
Console speed	An alternative console speed from 1200 to 115200

▼ To Configure OnBoard Boot

For more information about the fields in the “Boot Configuration” form, see Table 5-4, if needed.

1. Go to Settings → Boot configuration.

   The Boot Configuration form appears.

2. Enter the IP address of the OnBoard in the “OnBoard IP Address” field.
3. Accept or change the option in the “Watchdog Timer” field (either Inactive or Active).
4. Choose the desired image or “Network” from the “Unit boot from” menu.

5. If configuring network boot, do the following steps.
   a. Accept or change the filename of the network boot program in the "Network boot file name" field.

      The file must be in the `/tftpboot` directory on the TFTP server specified in Step b.

   b. Enter the IP address of the TFTP server in the "Server's IP address" field.

   c. Select a console speed from the "Console speed" pull-down menu.
6. Click "Save and apply changes."

Configuring an Alternate Help File Location

When an administrative user selects the Help option under Settings, a screen appears like the one shown in the following figure.

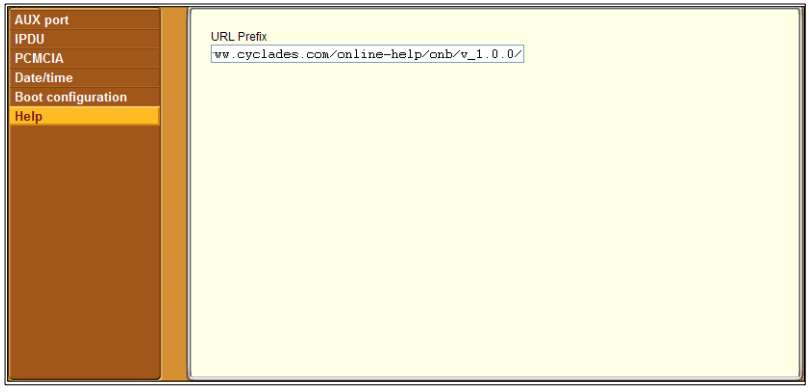


Figure 5-37: Settings → Help Screen

The Help button on the Web Manager looks for its help files in the location specified here. By default, the OnBoard help is located at the Cyclades web site at the specified URL: `www.cyclades.com/online-help/onb/v_1.0.0`.

If an OnBoard administrator downloads the help files from Cyclades onto another web server that is available to users, and then an administrative user can change the URL in the "URL Prefix" field to point to the Help button to the new location for the files.

▼ *To Specify a New Location for OnBoard Help Files*

1. Download the help files from `www.cyclades.com/online-help/onb/v_1.0.0` and install them on a publicly accessible web server.
2. Log into the Web Manager as admin, and go to Settings → Help.

   The Help configuration screen appears.
3. Enter the URL of the help files.
4. Click “Save and apply changes.”

Chapter 6
Web Manager “Config” Menu Options

This chapter describes the menu options available to administrative users under the “Config” top menu option.

For an overview of all the Web Manager features and menu options that are available for administrative users, see Chapter 2, “Web Manager Introduction,” if needed.

This chapter covers the topics in the following sections.

Options Under “Config”	Page 161
Configuring Devices	Page 163
Configuring Users and Groups	Page 169
Configuring Authentication	Page 178
Configuring Notifications	Page 194
Configuring Sensor Alarms	Page 201
Configuring SNMP	Page 209
Configuring Logging of System Messages (Syslogs)	Page 219
Configuring the Event Log Backend	Page 222
Selecting or Configuring a Security Profile	Page 224
Configuring the OnBoard’s Services	Page 229

This chapter provides the procedures listed in the following table.

To Add a Device	Page 166
To Sort the Device List Alphabetically	Page 168
To Create and Authorize a User for Device Management	Page 174

To Modify a User's Account	Page 175
To Create and Authorize a Group for Device Management	Page 177
To Configure a Kerberos Authentication Server	Page 181
To Configure an LDAP Authentication Server	Page 184
To Configure a NIS Authentication Server	Page 185
To Configure a Radius Authentication Server	Page 187
To Configure an SMB Authentication Server	Page 189
To Configure a TACACS+ Authentication Server	Page 191
To Configure an Authentication Method for OnBoard Logins	Page 193
To Configure SNMP Trap Notifications	Page 196
To Configure Pager Notifications	Page 198
To Configure an Email Notification	Page 200
To Begin Configuring a Sensor Alarm	Page 202
To Configure a Syslog Message Sensor Alarm Action	Page 204
To Configure an SNMP Trap Sensor Alarm Action	Page 206
To Configure a Pager Sensor Alarm Action	Page 208
To Configure an Email Sensor Alarm Action	Page 209
To Configure OnBoard SNMP Information	Page 211
To Configure SNMP for a Device	Page 217
To Configure the Syslog Destination and Message Filtering	Page 221
To Configure Event Logging for Connected Service Processors	Page 223
To Select the OnBoard's Security Profile	Page 229
To Configure Services	Page 230

Options Under “Config”

When an administrative user clicks the “Config” option in the top menu of the Web Manager, ten options appear in the left menu, as shown in the following figure.

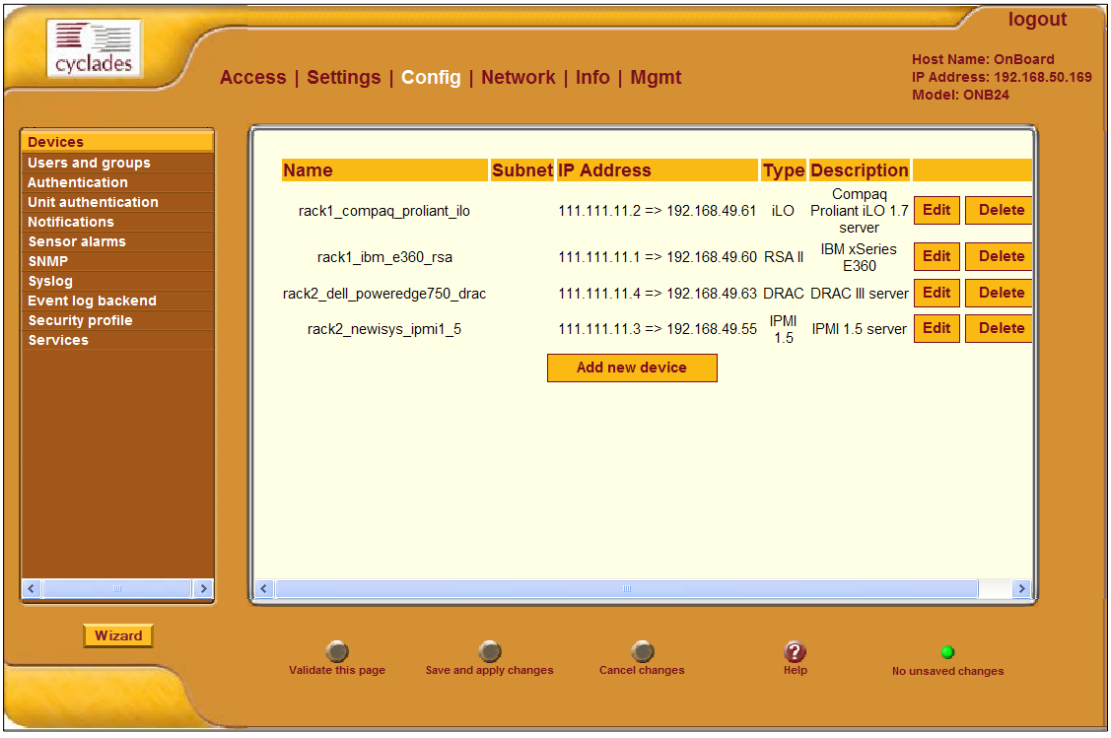


Figure 6-1: “Config” Menu Options

The following table lists the options that appear when an administrative user clicks “Config” and provides links to where the options are described.

Table 6-1: Options Under “Config”

Option	Where Described
Devices	“Configuring Devices” on page 163
Users and groups	“Configuring Users and Groups” on page 169
Authentication	“Configuring Authentication” on page 178

Table 6-1: Options Under “Config” (Continued)

Option	Where Described
Unit Authentication	“Configuring an Authentication Method for the OnBoard” on page 192
Notifications	“Configuring Notifications” on page 194
Sensor alarms	“Configuring Sensor Alarms” on page 201
SNMP	“Configuring SNMP” on page 209
Syslog	“Configuring SNMP” on page 209
Event log backend	“Configuring the Event Log Backend” on page 222
Security profile	“Selecting or Configuring a Security Profile” on page 224
Services	“Configuring the OnBoard’s Services” on page 229

Configuring Devices

When an administrative user goes to Config → Devices, a screen appears like the one shown in the following figure. As shown, entries appear for any configured devices, and “Edit” and Delete” buttons appear next to each device’s entry. The “Add new device” button always appears on the screen.

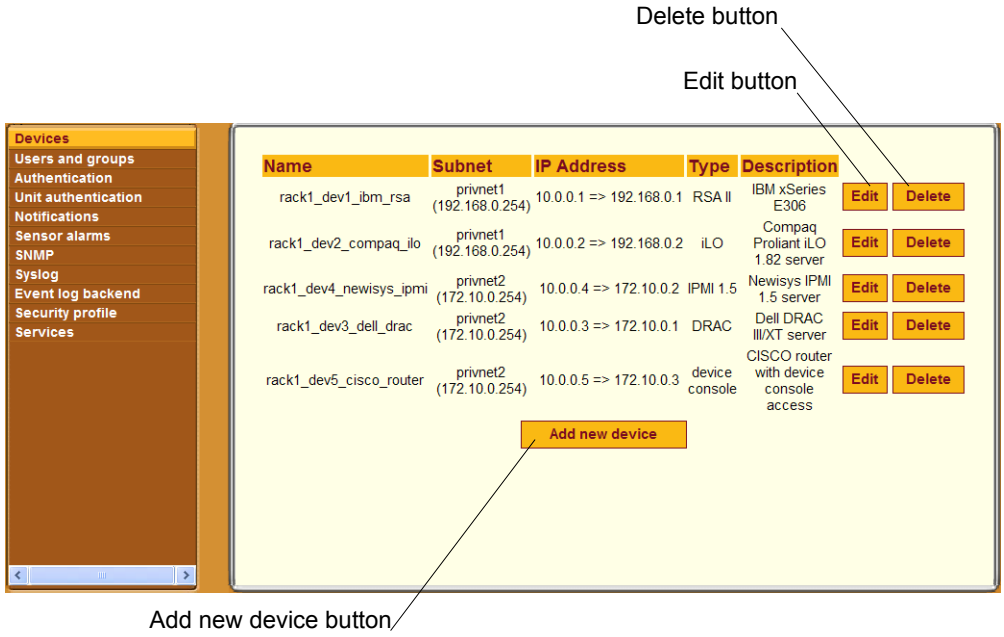


Figure 6-2: Config → Devices Screen

An administrative user can use the Config → Devices screen for configuring devices connected to the OnBoard. Clicking the “Add new device” or “Edit” buttons bring up a screen with fields shown in the following figure.

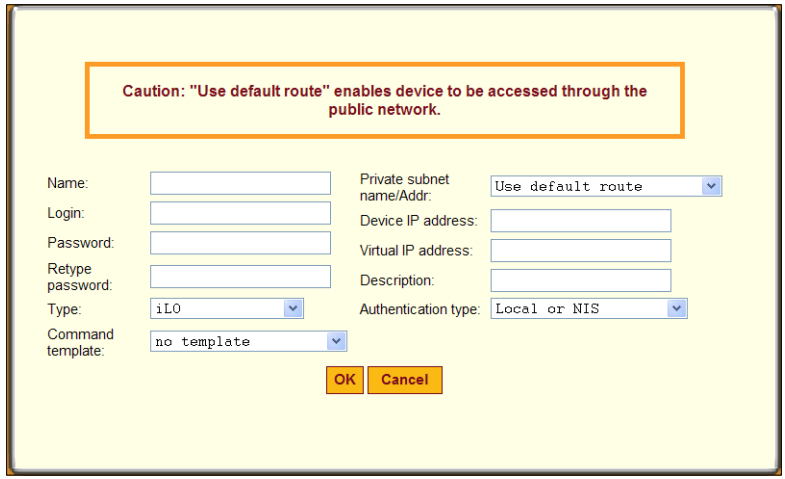


Figure 6-3: Fields in the "Add New Device" or "Edit" Dialog

Caution! All devices connected to the private Ethernet ports of the OnBoard must have a previously-configured private subnet name assigned. The Caution at the top of the dialog shown in Figure 6-3 is a reminder that if the default route is assigned instead of a private subnet, the device can only be accessed if it is connected to the public interface of the OnBoard, a highly unlikely scenario and not recommended.

Table 1-24, "Device Configuration Parameters," on page 58 lists the parameters that must be configured for each device.

The Web Manager displays devices in the order in which they are added. Alphabetical sorting is not available through the Web Manager. An OnBoard administrator can configure the Web Manager to display device lists in alphabetical order using the cycli utility. See "To Sort the Device List Alphabetically" on page 168.

Assigning a Device Type and Command Template

During configuration, each device must be assigned a device *type* and most devices must be assigned a *command template*.

The OnBoard administrator should not assign a command template when the device is either of the following two types of devices:

- Any IPMI-type device (IPMI devices are managed using `ipmitool` commands)
- Any device being configured only for Native IP access

Device Types

The following lists each of the defined SP and device types.

- iLO
- RSA II
- DRAC
- IPMI 1.5
- device console

Three additional custom types may be assigned, but only if OnBoard administrators have created customized scripts:

- `custom1`
- `custom2`
- `custom3`

Note: In most cases, the administrative user should not assign any of the custom device types to a device. Assign a `custom`*N* type to a device only if the default scripts and command templates cannot be made to work and only if an OnBoard administrator has created a custom expect script with the same number in its name. For details, see Appendix A, ‘Advanced Device Configuration” on page 309.

Command Templates

As mentioned elsewhere, command templates contain text commands that are used to interact with connected service processors/devices.

The following table lists the default command templates and describes the types of devices to which they apply. See "Understanding How the OnBoard Manages Communications With Devices" on page 311" for reasons why the default command templates may not work and for what to do if they do not work.

Table 6-2: Default Command Templates

Template	Type of Device
`devconsole.default`	Devices that support access to their consoles.
`drac.default`	DRAC type devices.
`ilo.default`	iLO type devices.
`rsa.default`	Some RSA II type devices.
`rsa.limited.default`	RSA II type devices that support only power commands through their command line interface.
`no template`	• IPMI type devices. • Any type device for which only Native IP access is being configured.

Also see "Command Templates" on page 321.

▼ *To Add a Device*

This procedure assumes the following prerequisites are complete.

- A private subnet has been created.
- An administrator has followed the procedure under "To Find Out if An Existing Command Template Works With a New Device" on page 317 to find out if a default command template works with the new device and to create a new command template if needed.
- You know the username and password pair that are used for logging into the service processor or device.

1. Log into the Web Manager as an administrative user.
2. Go to Config → Devices.
3. Click the "Add new device" button.

4. Enter a descriptive name for service processor or other type of connected device in the “Name” field.
5. Enter the username and password pair used for logging into the device in the “Login” and “Password” fields and retype the password in the “Retype password” field.
6. Select the device type from the “Type” pull-down menu:
   - iLO
   - RSA II
   - DRAC
   - IPMI 1.5
   - device console
   - custom 1
   - custom 2
   - custom 3
7. Select a command template or “no template” from the “Command template” pull-down menu.
8. Select a private subnet name from the “Private subnet name/Addr” field.
9. Enter the real IP address for the device in the “Device IP address” field.
10. If a virtual address has been configured, enter a virtual IP address for the device in the “Virtual IP address” field.
11. Enter a device description in the “Description” field.
12. Select an authentication type from the “Authentication type” pull-down menu.
13. Click OK.
14. Click “Save and apply changes.”

▼ *To Sort the Device List Alphabetically*

1. Log into the OnBoard command line as an administrative user or root.

```
OnBoard login: root
Password: password
```

2. Enter the `cycli` command.

```
[root@OnBoard root]# cycli
```

3. Make sure the primary Ethernet interface (`eth0`) is active.

```
cli> set onboard global sort server alpha
```

4. Save the changes.

```
cli> commit
```

5. Exit from the `cycli` utility.

```
cli> quit
```

6. Log out and bring up the Web Manager Config → Devices screen.

   The devices now display sorted alphabetically by name.

Configuring Users and Groups

When an administrative user goes to Config → Users and groups, a screen like the one shown in the following figure appears.

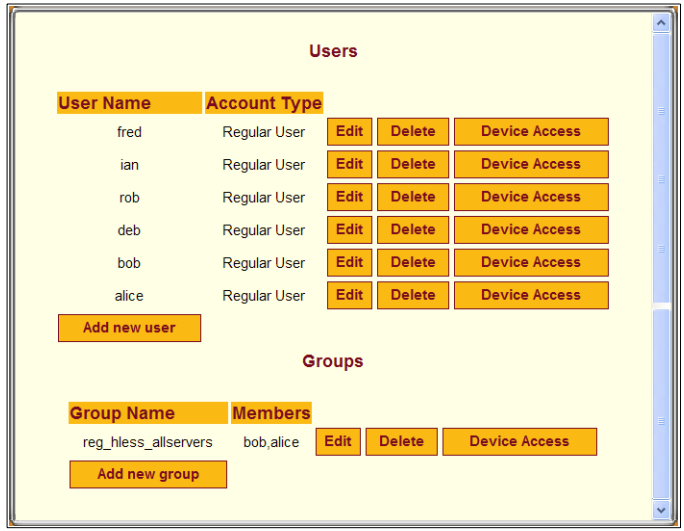


Figure 6-4: Config → Users and Groups Screen

The administrative user can use the “Config → Users and groups” screen for adding and configuring users and groups who can access devices through the OnBoard. The administrative user may also choose to add additional users who can administer the OnBoard as administrative users by adding them to the “admin” group.

Configuring Users

Clicking the “Add new user” or “Edit” buttons shown in Figure 6-4 brings up a screen with the fields shown in the following figure.

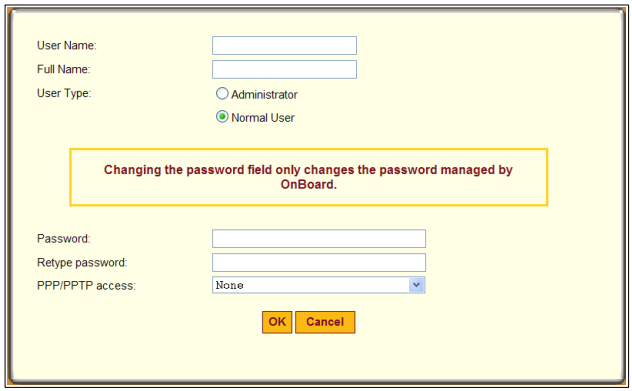


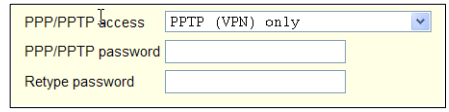
Figure 6-5: Add New User or Edit Dialog

Table 6-3 describes the parameters that can be set on the screens that appear when the “Add a regular user” option is selected.

Table 6-3: User Configuration Settings

Settings		Notes
User Name		Login name required for the user account.
Full name		Administratively-defined name to identify the user.
User Type	• Administrator • Normal User	Selecting the radio button next to “Administrator” adds the user to the “admin” group, which makes the user an administrative user who can perform OnBoard configuration.
Password		Password used for accessing the OnBoard.
Retype Password		As stated.

Table 6-3: User Configuration Settings (Continued)

Settings		Notes
• Sensors • Event log • Device Console	• Power • Service Processor Console • Native IP	Check any of the checkboxes to authorize the user to perform the selected device management actions
PPP/PPTP access	• None • PPP (dialup only) • PPTP (VPN only) • PPP (dialup) and PPTP (VPN)	Selecting PPP or PPTP for the user causes the two additional fields to display for setting the PPP or PPTP password, as shown in the following screen example: 

Clicking the “Delete” button shown in Figure 6-4 deletes the user without bringing up a confirmation dialog.

Clicking the “Device Access” button shown in Figure 6-4 brings up the “Edit *username*’s device access privileges” screen with fields shown in the following figure.

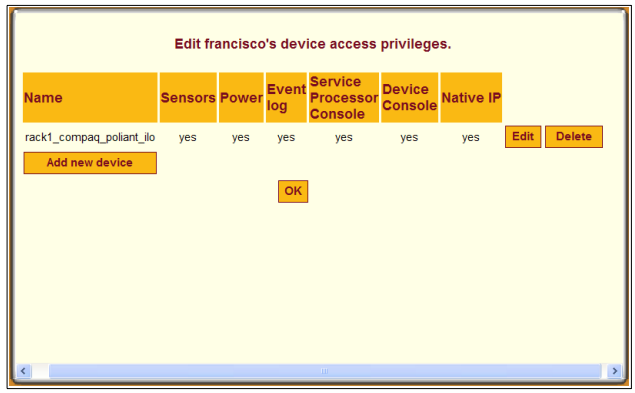


Figure 6-6: Add or Edit a User’s Device Access Dialog

If no configured devices remain to be assigned to the user, the “Add new device” button does not appear. Clicking the “Add new device” or “Edit”

buttons brings up a screen with the fields and menu options shown in the following figure.

Figure 6-7: Add New Device or Edit Device Dialog

On the dialog shown in Figure 6-7, the following device management actions are available to assign for the selected device to the selected user:

- Sensors
- Event log
- Device console
- Power
- Service processor console
- Native IP

Configuring Groups

Clicking the “Add new group” button or clicking the “Edit” button for an existing group brings up a screen with the fields shown in the following figure.

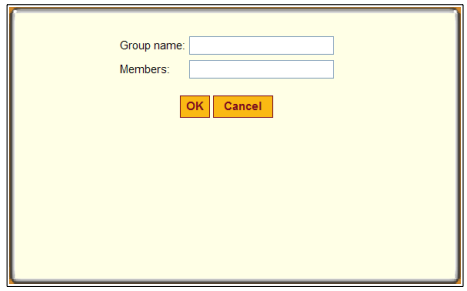


Figure 6-8: Add New Group or Edit Dialog

Clicking the “Delete” button shown in Figure 6-9 deletes the group without bringing up a confirmation dialog.

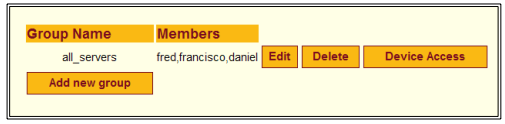


Figure 6-9: Group Configuration Buttons

Clicking the “Device Access” button shown in Figure 6-9 brings up the “Edit *groupname*’s device access privileges” screen with fields shown in the following figure.

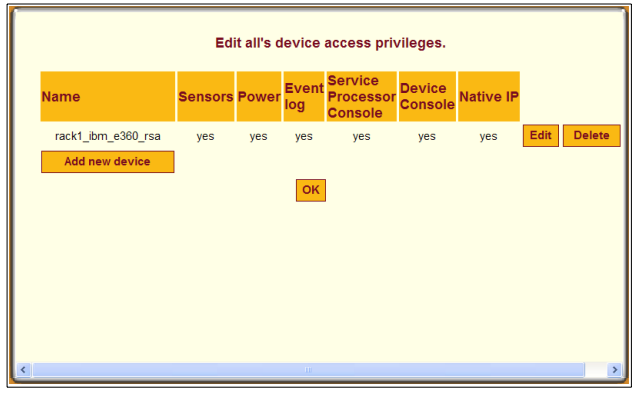


Figure 6-10: Add or Edit a Group's Device Access Dialog

If no configured devices remain to be assigned to the group, the "Add new device" button shown in Figure 6-10 does not appear. Clicking the "Add new device" button brings up a screen with the fields and menu options shown in the following figure.

Figure 6-11: Add New Device to a Group Dialog

▼ *To Create and Authorize a User for Device Management*

1. Log into the Web Manager as an administrative user.

   See "To Log Into the Web Manager" on page 75, if needed.

2. Go to Config → Users and groups.

3. To add a user, do the following steps.
   a. Click the “Add new user” button.
   b. Enter a username in the “User Name” field.
   c. Enter an identifying name and optional job description in the “Full Name” field.
   d. Select one of the radio buttons to choose a “User Type:”
   e. Enter a password in the “Password” field and re-enter it in the “Retype password” field.
   f. Select an option from the “PPP/PPTP access” pull-down menu:
   g. If you select any option except “None” from the “PPP/PPTP access” pull-down menu, enter a password in the “PPP/PPTP password” field and re-enter it in the “Retype password” field.
4. Assign device access to a user by performing the following steps.
   a. Click the “Device Access” button.
   b. Click the “Add new device” button.

      The “Adding access to a new device for *username*” screen appears.
   c. Select the device from the “New device” pull-down menu.
   d. Check the checkbox next to each device management action for which you wish to authorize the user to be able to perform on the selected device.
   e. Click OK.

      The “Edit *username*’s device access privileges” screen appears.
5. Click OK.
6. Click “Save and apply changes.”

▼ *To Modify a User’s Account*

1. Log into the Web Manager as an administrative user and go to Config → Users and groups.
2. Modify the user’s name, role, description, and PPP/PPTP access by performing the following steps.

a. Click the “Edit” button.

b. If desired, change the username in the “User Name” field.

c. If desired, change which radio button(s) is selected: “Administrator” or “Normal user.”

d. If desired, change the full name and optional job description in the “Full Name” field.

e. If desired, change the user’s password in the “Password” field and re-enter it in the “Retype password” field.

f. If desired, select an option or change which option is selected from the “PPP/PPTP access” pull-down menu:

g. If you select any option except “None” from the “PPP/PPTP access” pull-down menu, enter a password in the “PPP/PPTP password” field and re-enter it in the “Retype password” field.

h. Click OK.

3. Modify the user’s device access by performing the following steps.

a. Click the “Device Access” button.

b. Click the “Add new device” button.

The “Adding access to a new device for *username*” screen appears.

c. Select the device from the “New device” pull-down menu.

d. Check the checkbox next to each device management action for which you wish to authorize the user to be able to perform on the selected device.

e. Click OK.

The “Edit *username*’s device access privileges” screen appears.

4. Click OK.

5. Click “Save and apply changes.”

▼ *To Create and Authorize a Group for Device Management*

1. Log into the Web Manager as an administrative user and go to Config → Users and groups.
2. Add a group by performing the following steps.
   a. Click the “Add a new group” button.
   b. Enter a group name in the “Group Name” field.
   c. Enter one or more members in the “Members” field.
   d. Separate user names with commas and no spaces.
   e. Click OK.

      The “Edit *groupname*’s device access privileges” screen appears.
3. Assign device access to a group by performing the following steps.
   a. Click the “Device Access” button on the line with the group name.
   b. Click the “Add new device” button.

      The “Adding access to a new device for *groupname*” screen appears.
   c. Select the device from the “New device” pull-down menu.
   d. Check the checkbox next to each device management action for which you wish to authorize the group to be able to perform on the selected device.
   e. Click OK.

      The “Edit *groupname*’s device access privileges” screen appears.
4. Click OK.
5. Click “Save and apply changes.”

Configuring Authentication

The administrative user must decide whether to require authentication for logins into the OnBoard or into connected devices. If any other method than local is chosen, the administrative user must configure an authentication server for each method.

The following table lists the tasks for configuring authentication and where the tasks are documented using the Web Manager.

Table 6-4: Tasks for Authentication Configuration

Task	Where Documented
Configure authentication servers	"Configuring Authentication Servers" on page 179 • "Configuring a Kerberos Authentication Server" on page 180 • "Configuring an LDAP Authentication Server" on page 183 • "Configuring a NIS Authentication Server" on page 185 • "Configuring a Radius Authentication Server" on page 186 • "Configuring an SMB Authentication Server" on page 188 • "Configuring a TACACS+ Authentication Server" on page 190
Specify an authentication method for OnBoard logins.	"Configuring an Authentication Method for the OnBoard" on page 192
Specify authentication for devices.	"Configuring Devices" on page 163 "Selecting or Configuring a Security Profile" on page 224

Configuring Authentication Servers

The administrative user can use the Config → Authentication screen to configure all authentication servers to be used by the OnBoard or connected devices. When an administrative user goes to Config → Authentication, the screen shown in the following figure appears with the menu options shown for configuring authentication servers.

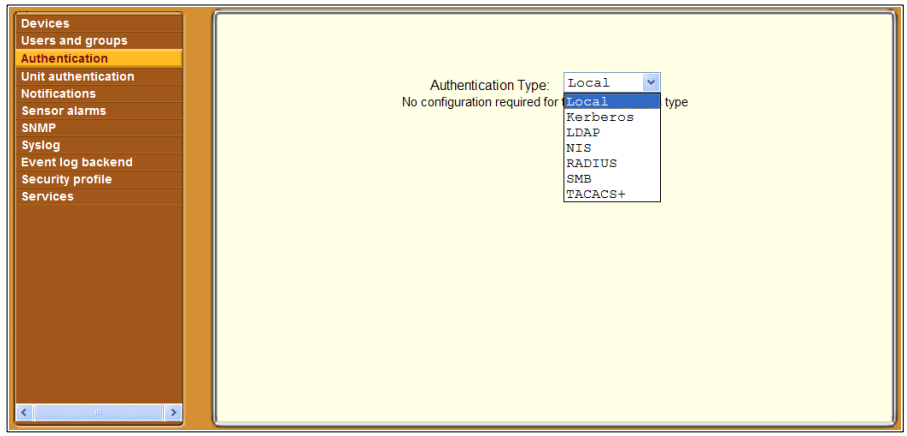


Figure 6-12: Default Config → Authentication Screen

The default authentication type is Local. If any other authentication method is selected, additional fields appear on the screen for specifying the information that is required to set up communications with an authentication server of the selected type.

Note: If NIS is configured as the authentication method for any device or for the OnBoard, NIS must be used as the only authentication method.

When the administrative user configures an authentication server on this page, the server is available to perform authentication checking for logins to the following:

- Any devices that are configured to use that authentication method

  See “Configuring Devices” on page 163 for how devices are assigned an authentication method on the Config → Devices screen.
- The OnBoard, if it is subsequently configured to use that authentication method.

See “Configuring an Authentication Method for the OnBoard” on page 192 for how the OnBoard is assigned an authentication method on the Config → Unit Authentication screen.

Configuring a Kerberos Authentication Server

When the administrative user goes to Config → Authentication or Config → Unit Authentication and selects Kerberos from the “Authentication Type” pull-down menu, the fields shown in the following figure appear. If a Kerberos authentication server has not previously been configured, the fields are empty.

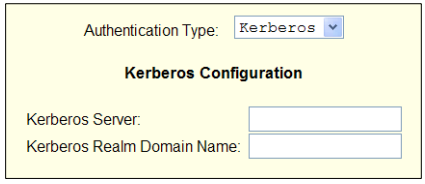


Figure 6-13: Config → Authentication: Kerberos

If the Kerberos authentication server (which is also referred to as a Key Distribution Center, or KDC) has previously been configured in either of the authentication configuration screens, the fields are filled in with the previously-configured values.

Before configuring a Kerberos server, the administrative user must obtain the needed information from the server’s administrator. The administrative user enters the information in the following two fields, which display when the Kerberos authentication type is selected:

- Kerberos Server IP address
- Kerberos Realm Domain Name

Caution! The Kerberos KDC rejects tickets when the timestamp on an authentication request from a host is not within the maximum clock skew time specified in the KDC’s `hdc.conf` file. Therefore, it is essential for the time on the OnBoard to be synchronized with the time on the KDC.

▼ *To Configure a Kerberos Authentication Server*

Perform this procedure to configure an authentication server when the OnBoard or any of its connected devices is to use the Kerberos authentication method or any of its variations (Kerberos, Local/Kerberos, Kerberos/Local, or Kerberos Down/Local).

Before starting this procedure, find out the following information from the Kerberos server's administrator:

- Kerberos Server IP address
- Kerberos Realm Domain Name

Also, work with the Kerberos server's administrator to ensure that following types of accounts are set up on the Kerberos server and that the administrators of the OnBoard and connected devices know the passwords assigned to the accounts:

- An account for "admin" or other administrative user.
- If Kerberos authentication is specified for the OnBoard, accounts for all users who need to log into the OnBoard to administer connected devices.
- If Kerberos authentication is specified for devices, accounts for users who need access to connected devices

1. Log into the Web Manager as an administrative user.
2. Make sure entries for the OnBoard and the Kerberos server exist in the OnBoard's `/etc/hosts` file.
   a. Go to Network → Host Table.

      The "Host Table" form appears.

   b. Add an entry for OnBoard (if needed) and an entry for the Kerberos server.

      i. Click the "Add new host" button.

      ii. Enter the address in the "IP Address" field.

      iii. Enter the name in the "Name" field.

      iv. If desired, enter an optional alias in the "Alias" field.

      v. Click OK.

vi. Click “Save and apply changes.”

3. Make sure that timezone and time and date settings are synchronized between the OnBoard and on the Kerberos server.

Note: Kerberos authentication depends on time synchronization. Time and date synchronization is most easily achieved by setting both the OnBoard and the Kerberos server to use the same NTP server.

---

   a. Follow the procedure under “To Configure System Date and Time” on page 151 to set the timezone, date, and time.

   b. Work with the authentication server’s administrator to synchronize the time and date between the OnBoard and the server.

4. Go to Config → Authentication and select Kerberos from the “Authentication Type” pull-down menu.

   The Kerberos configuration fields display.

5. Enter the IP address of the Kerberos server in the “Kerberos Server IP address” field.

6. Enter the domain name of the Kerberos realm in the “Kerberos Realm Domain Name” field.

7. Click “Save and apply changes.”

Configuring an LDAP Authentication Server

When an administrative user goes to Config → Authentication or Config → Unit Authentication and selects LDAP from the "Authentication Type" pull-down menu, the fields shown in the following figure appear. If an LDAP authentication server has not previously been configured, the fields are empty.

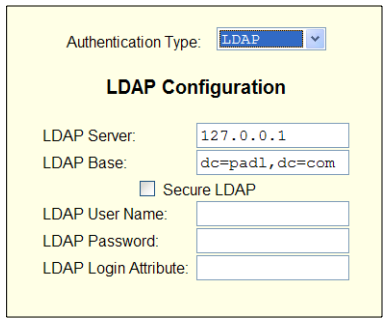


Figure 6-14: Config → Authentication: LDAP

If the LDAP authentication server has previously been configured, the fields are filled in with the previously-configured values.

To configure an LDAP server, the administrative user must obtain the needed information about the LDAP server from the server's administrator and fill in the fields and check the checkbox, as desired. The following fields and checkbox display when the LDAP authentication type is selected:

- LDAP Server IP address
- LDAP Base—The distinguished name of the search base
- Secure LDAP checkbox

You can enter information in the following two fields, but an entry is not required:

- LDAP User Name
- LDAP Login Attribute

▼ To Configure an LDAP Authentication Server

Perform this procedure to identify an authentication server when the OnBoard or any of its connected devices is to use the LDAP authentication method or any of its variations (Local/LDAP, LDAP/Local, or LDAP Down/Local).

Work with the LDAP server's administrator to ensure that following types of accounts are set up on the LDAP server and that the administrators of the OnBoard and connected devices know the passwords assigned to the accounts:

- An account for "admin" or other administrative user.
- If LDAP authentication is specified for the OnBoard, accounts for all users who need to log into the OnBoard.
- If LDAP authentication is specified for devices, accounts for users who need access to the connected devices.

1. Log into the Web Manager as an administrative user.
2. Go to Config → Authentication and select LDAP from the "Authentication Type" pull-down menu.

   The "LDAP" form displays with "LDAP Server" and "LDAP Base" fields filled in from the current values in the `/etc/ldap.conf` file.
3. Supply the IP address of the LDAP server in the "LDAP Server" field.
4. If the LDAP authentication server uses a different distinguished name for the search base than the one displayed in the "LDAP" Base field, change the definition.

   The default distinguished name is "dc," as in `dc=`*`value`*`,dc=`*`value`*. For example, if the distinguished name on the LDAP server is "o," then replace `dc` in the base field with `o`, as in `o=`*`value`*`,o=`*`value`*`.`
5. Replace the default domain name with the name of your LDAP domain.

   For example, for the LDAP domain name cyclades.com, the correct entry is: `dc=cyclades,dc=com`.
6. Click "Save and apply changes."

   The changes are stored in `/etc/ldap.conf` on the OnBoard.

Configuring a NIS Authentication Server

When an administrative user goes to Config → Authentication and selects NIS from the "Authentication Type" pull-down menu, the fields shown in the following figure appear.

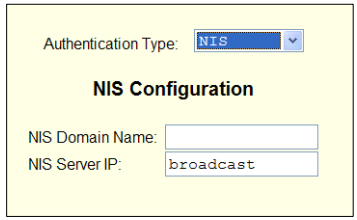


Figure 6-15: Config → Authentication: NIS

The administrative user must obtain the needed information about the NIS server from the server's administrator and configure the server by filling in these fields that display when the NIS authentication type is selected:

- NIS Domain Name
- NIS Server IP

Note: If you select NIS authentication for the OnBoard or for any device, NIS must be used as the only authentication method for the OnBoard and all devices.

▼ To Configure a NIS Authentication Server

Perform this procedure to identify the authentication server when the OnBoard or any of its connected devices is to use the NIS authentication method (Local/NIS or NIS/Local).

Work with the NIS server's administrator to ensure that following types of accounts are set up on the NIS server and that the administrators of the

OnBoard and connected devices know the passwords assigned to the accounts:

- An account for “admin”
- If NIS authentication is specified for the OnBoard, accounts for all users who need to log into the OnBoard.
- If NIS authentication is specified for devices, accounts for users who need access to the connected devices.

1. Log into the Web Manager as an administrative user.
2. Go to Config → Authentication and select NIS from the “Authentication Type” pull-down menu.

   The “NIS” fields display.
3. Enter the NIS domain name in the “NIS Domain Name” field.
4. Enter the IP address of the NIS server in the “NIS Server IP” field.
5. Click “Save and apply changes.”

Configuring a Radius Authentication Server

When an administrative user goes to Config → Authentication and selects Radius from the “Authentication Type” pull-down menu, the fields shown in the following figure appear.

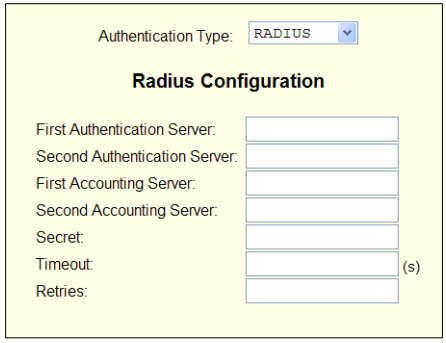


Figure 6-16: Config → Authentication: Radius

The administrative user must obtain the needed information about the Radius server from the server's administrator and configure the server by filling in these fields that display when the Radius authentication type is selected:

- First Authentication Server
- Second Authentication Server
- First Accounting Server
- Second Accounting Server
- Secret
- Timeout(s)
- Retries

▼ *To Configure a Radius Authentication Server*

Perform this procedure to identify the authentication server when the OnBoard or any of the connected devices is to use the Radius authentication method or any of its variations (Local/Radius, Radius/Local, or Radius Down/Local).

Work with the Radius server's administrator to ensure that following types of accounts are set up on the Radius server and that the administrators of the OnBoard and connected devices know the passwords assigned to the accounts:

- An account for "admin" or other administrative user.
- If Radius authentication is specified for the OnBoard, accounts for all users who need to log into the OnBoard.
- If Radius authentication is specified for devices, accounts for users who need access to the connected devices.

1. Log into the Web Manager as an administrative user.
2. Go to Config → Authentication and select Radius from the "Authentication Type" pull-down menu.
3. Enter the IP address of the first or only authentication server in the "First Authentication Server" field.
4. Optional: Enter the IP address of a second authentication server in the "Second Authentication Server" field.
5. Enter the secret in the "Secret" field.

6. Enter one or more timeout values in the “Timeout” field.
7. Enter a number of retries in the “Retries” field.
8. Click “Save and apply changes.”

Configuring an SMB Authentication Server

When the administrative user goes to Config → Authentication and selects SMB from the “Authentication Type” pull-down menu, the fields shown in the following figure appear.

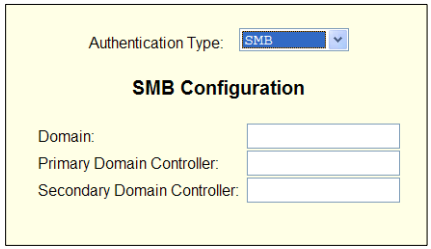


Figure 6-17: Config → Authentication: SMB

The administrative user must obtain the needed information about the SMB server from the server’s administrator and configure the server by filling in these fields that display when the SMB authentication type is selected:

- Domain
- Primary Domain Controller
- Secondary Domain Controller

▼ *To Configure an SMB Authentication Server*

Perform this procedure to identify the authentication server when the OnBoard or any of the connected devices is to use the SMB authentication method or any of its variations (Local/SMB, SMB/Local, or SMB Down/Local).

Work with the SMB server's administrator to ensure that following types of accounts are set up on the SMB server and that the administrators of the OnBoard and connected devices know the passwords assigned to the accounts:

- An account for "admin" or other administrative user.
- If SMB authentication is specified for the OnBoard, accounts for all users who need to log into the OnBoard.
- If SMB authentication is specified for devices, accounts for users who need access to the connected devices.

1. Log into the Web Manager as an administrative user.
2. Go to Config → Authentication and select SMB from the "Authentication Type" pull-down menu.
3. Enter the SMB domain name in the "Domain" field.
4. Enter the IP address of the primary domain controller in the "Primary Domain Controller" field.
5. Enter the IP address of the secondary domain controller in the "Secondary Domain Controller" field.
6. Click "Save and apply changes."

Configuring a TACACS+ Authentication Server

When the administrative user goes to Config → Authentication and selects TACACS+ from the "Authentication Type" pull-down menu, the fields shown in the following figure appear.

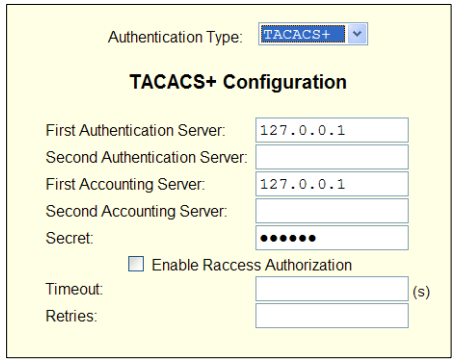


Figure 6-18: Config → Authentication: TACACS+

The administrative user must obtain the needed information about the TACACS+ server from the server's administrator. The administrative user must configure the server by filling in these fields or choosing whether to check or leave unchecked the checkbox that displays when the TACACS+ authentication type is selected:

- First Authentication Server
- Second Authentication Server
- First Accounting Server
- Second Accounting Server
- Secret
- Enable Raccess Authorization
- Timeout(s)
- Retries

▼ *To Configure a TACACS+ Authentication Server*

Perform this procedure to identify the authentication server when the OnBoard or any of the connected devices is to use the TACACS+ authentication method or any of its variations (Local/TACACS+, TACACS+/Local, or TACACS+ Down/Local).

Work with the TACACS+ server's administrator to ensure that following types of accounts are set up on the TACACS server and that the administrators of the OnBoard and connected devices know the passwords assigned to the accounts:

- An account for "admin" or other administrative user.
- If TACACS+ authentication is specified for the OnBoard, accounts for all users who need to log into the OnBoard.
- If TACACS+ authentication is specified for devices, accounts for users who need access to the connected devices.

1. Log into the Web Manager as an administrative user.
2. Go to Config → Authentication and select TACACS+ from the "Authentication Type" pull-down menu.
3. Enter the IP address of the first authentication server in the "First Authentication Server" field.
4. Enter the IP address of a second authentication server in the "Second Authentication Server" field.
5. Enter the IP address of the first accounting server in the "First Accounting Server" field.
6. Enter the IP address of the second accounting server in the "Second Accounting Server" field.
7. Enter the secret in the "Secret" field.
8. Check or leave unchecked the "Enable Raccess Authorization" checkbox.
9. Enter one or more timeout values in the "Timeout" field.
10. Enter a number of retries in the "Retries" field.
11. Click "Save and apply changes."

Configuring an Authentication Method for the OnBoard

When an administrative user goes to Config → Unit Authentication, the screen shown in the following figure appears. The administrative user uses this screen to configure the authentication method that applies when anyone attempts to log into the OnBoard.

Figure 6-19: Default Config → Authentication Screen

By default Local authentication is in effect, and no configuration is required.

The following figure shows the authentication methods available for OnBoard logins.

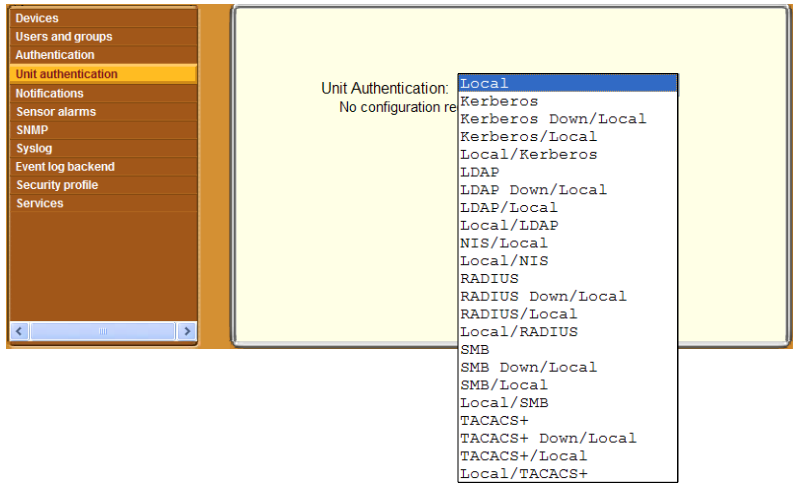


Figure 6-20: Default Config → Unit Authentication Screen With Menu Options

When an authentication method is selected from the menu, additional configuration fields appear. If an authentication server has already been configured for the selected method, the fields contain the appropriate information. If the fields are empty, the administrative user needs to configure the authentication server for the selected method, as described under “Configuring Authentication” on page 178.

▼ *To Configure an Authentication Method for OnBoard Logins*

Perform this procedure to configure an authentication method for logins into the OnBoard. This procedure assumes that an authentication server exists and has been configured as described under “Configuring Authentication” on page 178.

1. Log into the Web Manager as an administrative user.
2. Go to Config → Unit Authentication.

3. Select the desired authentication type from the “Authentication Type” pull-down menu.
4. Click “Save and apply changes.”

Configuring Notifications

When an administrative user goes to Config → Notifications, the screen shown in the following figure appears. The administrative user can use this screen for defining alarm triggers to generate notifications when they occur. The administrative user specifies the notices to be sent by one of the following methods:

- SNMP trap
- Pager
- Email

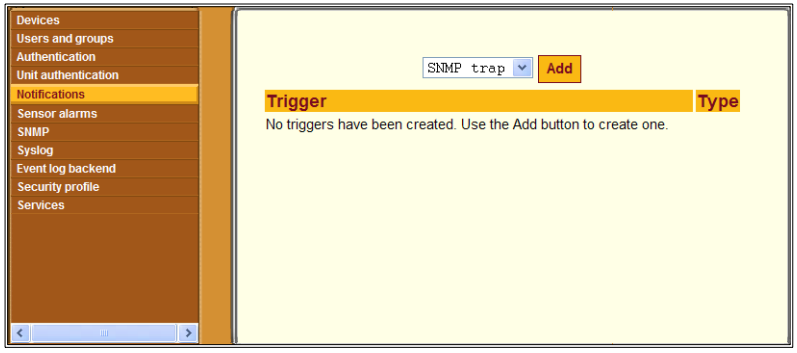


Figure 6-21: Default Config → Notifications Screen

The screen shown in Figure 6-21 is the default screen with no triggers listed.

To configure a notification, the administrative user clicks the “Add” button after selecting one of the notification methods from the menu. The screen that appears has different fields and menu options depending on which notification method was selected.

Configuring SNMP Trap Notifications

The following figure shows the fields that appear when “SNMP trap” is selected and the “Add” button is clicked on the Config → Notifications screen.

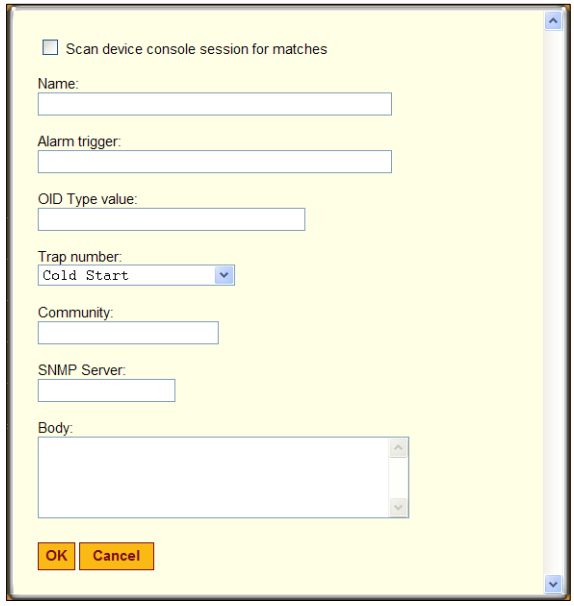


Figure 6-22: Config → Notifications: SNMP Trap Add Dialog

If the Simple Network Management Protocol (SNMP) service is enabled on the OnBoard, the OnBoard administrator can use the dialog shown in Figure 6-22 to send notifications about significant events or traps to an SNMP management application, such as HP Openview, Novell NMS, IBM NetView, or Sun Net Manager. The SNMP trap notification method dialog has the fields shown in the following table.

Table 6-5: Fields for Configuring an SNMP Trap Notification

Field or Menu Name	Notes
Scan device console session for matches	As stated
Name	The name for the trigger

Table 6-5: Fields for Configuring an SNMP Trap Notification (Continued)

Field or Menu Name	Notes
Alarm trigger	The event you want to trigger a notification
OID Type value	The number of the OID type value
Trap number	Cold Start
	Warm Start
	Link Down
	Link Up
	Auth Failure
	EGP Neighbor Loss
	Enterprise Specific
Community	The community name is sent in every communication between the client and the server, and the community name must be correct before requests are allowed.
SNMP Server	The SNMP server's IP address or DNS name.
Body	The text you want sent in the trap message.

▼ *To Configure SNMP Trap Notifications*

Perform this procedure to configure an alarm trigger and a SNMP trap notification to be sent if the specified alarm trigger occurs.

1. Log into the Web Manager as an administrative user and go to Config → Notifications.
2. Select "SNMP trap" from the pull-down menu.
3. Check or leave unchecked the checkbox next to "Scan device console session for matches."
4. Enter a name for the trigger in the "Name" field.
5. Enter an event to trigger the alarm in the "Alarm trigger" field.

6. Enter an OID type number in the “OID Type value” field.
7. Select one of the trap designators from the “Trap number” pull-down menu.
8. Enter a community name in the “Community” field.
9. Enter an SNMP server IP address or DNS name in the “SNMP server” field.
10. Enter any desired text in the “Body” field.
11. Click OK.
12. Click “Save and apply changes.”

Configuring Pager Notifications

The following figure shows the fields that appear when “Pager” is selected and the “Add” button is clicked on the Config → Notifications screen.

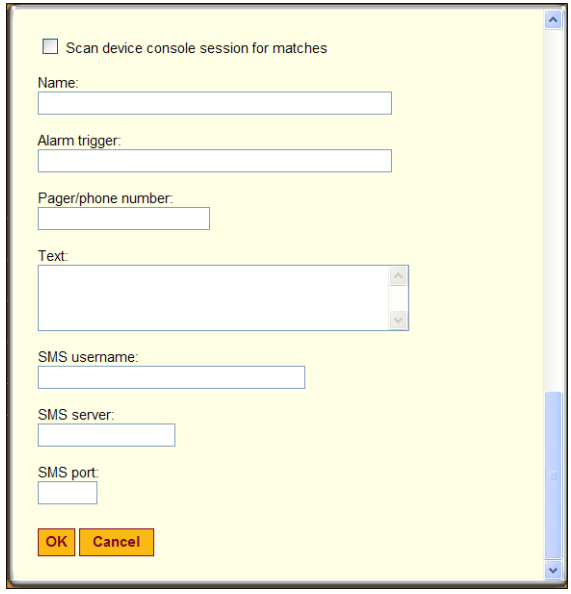


Figure 6-23: Config → Notifications: Pager Add Dialog

The values you need to complete the form and associated dialog boxes are explained in the following table.

Table 6-6: Fields for Configuring a Pager Notification

Field or Menu Name	Notes
Scan device console session for matches	As stated
Name	The name for the trigger
Alarm trigger	The event that triggers a notification
Pager/phone number	The pager or phone number to receive the notification
Text	The text to be sent in the trap message
SMS username	The Short Message Services (SMS) user name
SMS server	The SMS server's IP address or DNS name
SMS port	The SMS port number

▼ *To Configure Pager Notifications*

Perform this procedure to configure an alarm trigger and a pager notification to be sent if the specified alarm trigger occurs.

1. Log into the Web Manager as an administrative user and go to Config → Notifications.
2. Select "Pager" from the pull-down menu.
3. Check or leave unchecked the checkbox next to "Scan device console session for matches."
4. Enter a name for the notification in the "Name" field.
5. Enter an event to trigger the alarm in the "Alarm trigger" field.
6. Enter a pager or phone number in the "Pager/phone number" field.
7. Enter the desired text in the "Text" field.
8. Enter a username in the "SMS username" field.

9. Enter the IP address for an SMS server in the “SMS server” field.
10. Enter an SMS port in the “SMS port” field.
11. Click OK.
12. Click “Save and apply changes.”

Configuring Email Notifications

The following figure shows the fields that appear when the Email option is selected and the Add button is clicked.

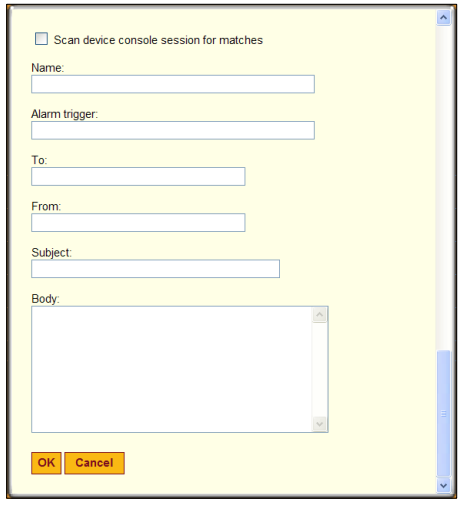


Figure 6-24: Default Config → Notifications: Email Add Dialog

The email notification method dialog has the fields shown in the following table.

Table 6-7: Fields for Configuring an Email Notification

Field or Menu Name	Notes
Scan device console session for matches	As stated
Name	The name for the trigger
Alarm trigger	The event that triggers a notification

Table 6-7: Fields for Configuring an Email Notification (Continued)

Field or Menu Name	Notes
To	The email address of the user account to receive the notification
From	The sender's email address
Subject	Summary text to describe the event triggering the email
Body	Description of the event

▼ *To Configure an Email Notification*

Perform this procedure to configure an alarm trigger and an email notification to be sent if the specified alarm trigger occurs.

1. Log into the Web Manager as an administrative user and go to Config → Notifications.
2. Select "Email" from the pull-down menu.
3. Check or leave unchecked the checkbox next to "Scan device console session for matches."
4. Enter a name for the notification in the "Name" field.
5. Enter an event to trigger the alarm in the "Alarm trigger" field.
6. Enter a destination email address in the "To" field.
7. Enter a source email address in the "From" field.
8. Enter a subject that describes the alarm trigger in the "Subject" field.
9. Enter the desired text for the email message in the "Body" field.
10. Click OK.
11. Click "Save and apply changes."

Configuring Sensor Alarms

When an administrative user goes to Config → Sensor alarms, the screen shown in the following figure appears. The administrative user can use this screen to configure the OnBoard to check sensor readings from service processors and to configure alarms to be sent if the sensor readings are not within certain specified values.

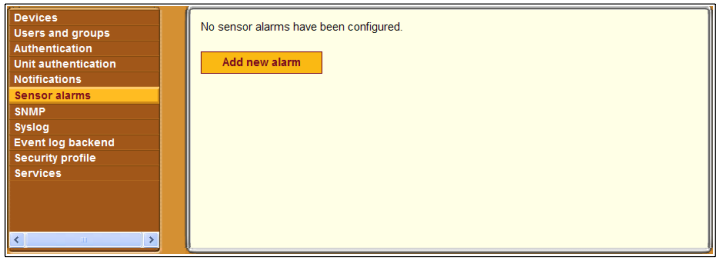


Figure 6-25: Default Config → Sensor Alarms Screen

Figure 6-25 shows the screen as it appears when no alarms are configured.

Figure 6-26 shows the screen as it appears when the “Add new alarm” button is clicked on the screen that is shown in Figure 6-25. As shown, by default, the “Syslog message” option is selected from the “Action” menu.

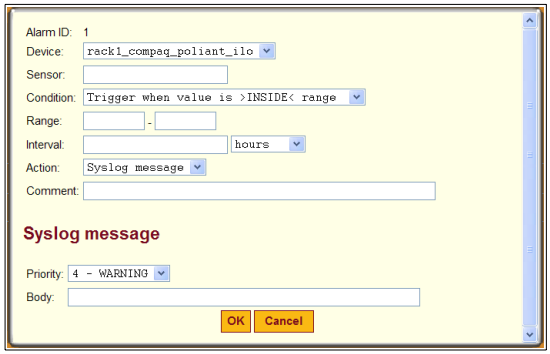


Figure 6-26: Default Config → Sensor Alarms Screen

The following table shows the fields for configuring sensor alarms.

Table 6-8: Fields for Configuring Sensor Alarms

Field or Menu Name	Description
Device	All configured devices
Sensor	The name of the sensor.
Condition	• Trigger when value is >INSIDE< range • Trigger when value is <OUTSIDE> range • Trigger when value CHANGES
Range	Chosen by the administrator
Interval	A polling interval chosen by the administrator: a time in minutes or hours
Action	• Syslog message • SNMP trap • Pager • Email
Comment	Any desired comment to identify the source of the alarm

▼ *To Begin Configuring a Sensor Alarm*

Perform this procedure to monitor a sensor on a specific devices and configure an alarm trigger and a notification to be sent if the specified alarm trigger occurs.

1. Log into the Web Manager as an administrative user and go to Config → Sensor Alarms.
2. Select a device from the “Device” pull-down menu.
3. Specify the sensor to monitor in the “Sensor” field.
4. Select a condition to trigger the sensor alarm from the “Condition” pull-down menu.
5. When the condition is inside or outside a range, specify the range in the “Range” fields.

6. Specify a polling interval and choose “minutes” or “hours” from the “Interval” pull-down menu.
7. Select the desired notification action from the “Action” pull-down menu.
8. Enter a comment, if desired, in the “Comment” field.
9. Go to the appropriate procedure from the following table, depending on which option is selected from the “Action” menu in Step 7.

To Configure a Syslog Message Sensor Alarm Action	Page 204
To Configure an SNMP Trap Sensor Alarm Action	Page 206
To Configure a Pager Sensor Alarm Action	Page 208
To Configure an Email Sensor Alarm Action	Page 209

Configuring a “Syslog Message” Sensor Alarm Action

The following figure shows the fields that appear when “Syslog Message” is selected on the “Action” menu on the Config → Sensor Alarms screen that is shown in Figure 6-26.

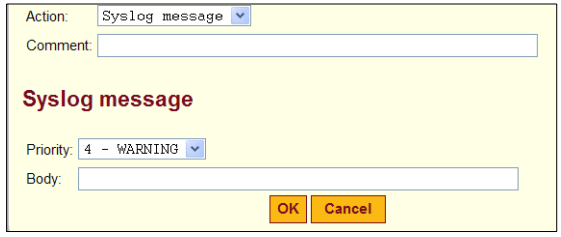


Figure 6-27: Config → Sensor Alarms Syslog Message Fields

The following table describes the fields in Figure 6-27.

Table 6-9: Fields for Configuring Syslog Message Sensor Alarms

Field or Menu Name	Notes
Priority	• 0 - EMERG • 1 - ALERT • 2 - CRIT • 3 - ERR • 4 - WARNING • 5 - NOTICE • 6 - INFO • 7 - DEBUG
Body	Any desired text to include with the syslog message.

▼ *To Configure a Syslog Message Sensor Alarm Action*

1. Perform Step 1 through Step 8 in the procedure "To Begin Configuring a Sensor Alarm" on page 202, selecting "Syslog message" from the "Action" menu in Step 7.
2. Select a priority from the "Priority" menu.
3. Enter text as desired in the "Body" field.
4. Click OK.
5. Click "Save and apply changes."

Configuring the "SNMP Trap" Sensor Alarm Action

The following figure shows the fields that appear when "SNMP trap" is selected on the "Action" menu on the Config → Sensor Alarms screen that is shown in Figure 6-26.

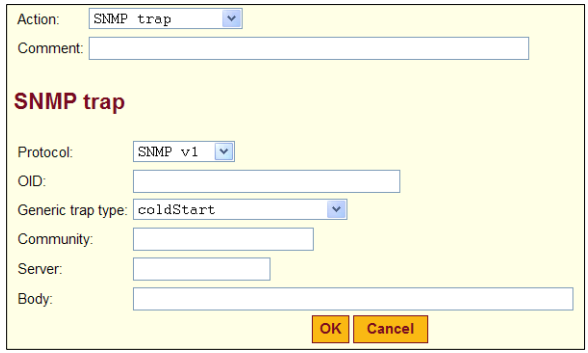


Figure 6-28: Config → Sensor Alarms SNMP Trap Fields

The following table describes the fields in Figure 6-28.

Table 6-10: Fields for Configuring a SNMP Trap Sensor Alarms

Field or Menu Name	Description
Protocol	• SNMP v1 • SNMP v2c • SNMP v3
OID	Object Identifier. Each managed object has a unique identifier.
Generic trap type	coldStart warmStart linkDown linkUp authenticationFailure egpNeighborLoss enterpriseSpecific

Table 6-10: Fields for Configuring a SNMP Trap Sensor Alarms (Continued)

Field or Menu Name	Description
Community	SNMP v1 and v2 only. The community name is sent in every communication between the client and the server, and the community name must be correct before requests are allowed. Communities are further defined by the type of access specified under "Permission": either read only or read write. The most common community is "public" and it should not be used because it is so commonly known. By default, the public community cannot access SNMP information on the OnBoard.
Server	IP address of the SNMP server
Body	Administrator-chosen text

▼ *To Configure an SNMP Trap Sensor Alarm Action*

1. Perform Step 1 through Step 8 in the procedure "To Begin Configuring a Sensor Alarm" on page 202, selecting "SNMP trap" from the "Action" menu in Step 7.
2. Select a protocol from the "Protocol" menu.
3. Enter the OID in the "OID" field.
   a. Select a trap type from the "Generic trap type" field.
   b. If either v1 or v2 is selected in Step a, enter the name of a community in the "Community" field.
   c. If v3 is selected in Step a, perform the following steps.
      i. Enter the username required for authentication in the "User" field.
      ii. Choose an authentication type from the "Authentication Type" pull-down menu.
      iii. Enter the authentication password in the "Password" field.
      iv. Select an encryption method from the "Encryption" pull-down menu.

v. Enter the appropriate password for the encryption method in the "Crypt pass" field.

d. Enter the IP address or DNS-resolvable name of the SNMP server in the "Server" field.

e. Enter any desired text in the "Body" field.

4. Click OK.

Configuring a "Pager" Sensor Alarm Action

The following figure shows the fields that appear when "Pager" is selected on the "Action" menu on the Config → Sensor Alarms screen that is shown in Figure 6-26.

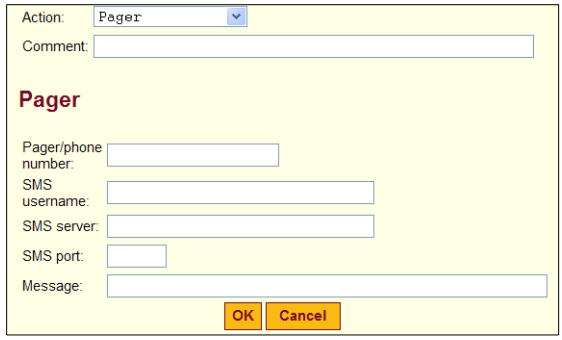


Figure 6-29: Config → Sensor Alarms Pager Message Fields

The following table describes the fields in Figure 6-27.

Table 6-11: Fields for Configuring Syslog Message Sensor Alarms

Field or Menu Name	Notes
Pager/phone number	Pager or phone number.
SMS username	SMS user name.
SMS server	SMS server IP address.
SMS port	Port number.
Message	Any desired text to include with the pager message.

▼ To Configure a Pager Sensor Alarm Action

1. Perform Step 1 through Step 8 in the procedure “To Begin Configuring a Sensor Alarm” on page 202, selecting “Pager” from the “Action” menu in Step 7.
2. Enter the phone number of the pager or phone to be contacted in the “Pager/phone number” field.
3. Enter the user name required for authentication in the “SMS username” field.
4. Enter the IP address of the SMS server in the “SMS server” field.
5. Enter the SMS port number in the “SMS port” field.
6. Enter any desired message in the “Message” field.
7. Click OK.
8. Click “Save and apply changes.”

Configuring an “Email” Sensor Alarm Action

The following figure shows the fields that appear when “Email” is selected on the “Action” menu on the Config → Sensor Alarms screen that is shown in Figure 6-26.

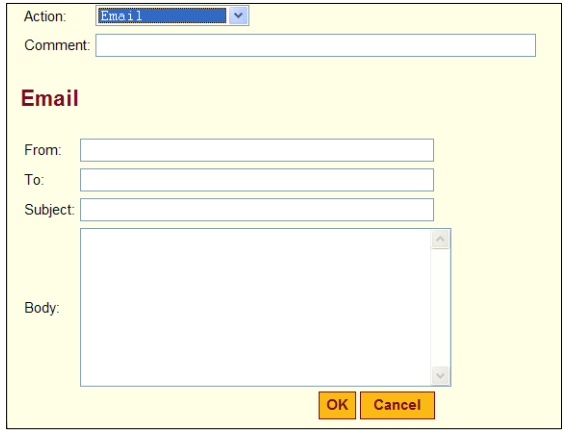


Figure 6-30: Config → Sensor Alarms Email Message Fields

The following table describes the fields in Figure 6-27.

Table 6-12: Fields for Configuring Email Sensor Alarms

Field or Menu Name	Notes
From:	Identifies the sender, for example root@OnBoard
To:	Designates who is to receive of the email
Subject:	Identifies the source of the message, for example: “Alarm: Sensor Error from rack1_dev2_ilo.”
Body	Any desired text to include with the email message.

▼ *To Configure an Email Sensor Alarm Action*

1. Perform Step 1 through Step 8 in the procedure “To Begin Configuring a Sensor Alarm” on page 202, selecting “Email” from the “Action” menu in Step 7.
2. Enter the sender’s email address in the “From” field.
3. Enter the recipient’s email address in the “To” field.
4. Enter a string that identifies the alarm in the “Subject” field.
5. Enter an explanatory message for the alarm in the “Body” field.
6. Click OK.
7. Click “Save and apply changes.”

Configuring SNMP

The OnBoard administrator can use this screen to configure Simple Network Management Protocol (SNMP) access for the OnBoard and for connected devices.

Figure 6-31 shows the screen that appears when the “SNMP” option is selected from the Config menu.

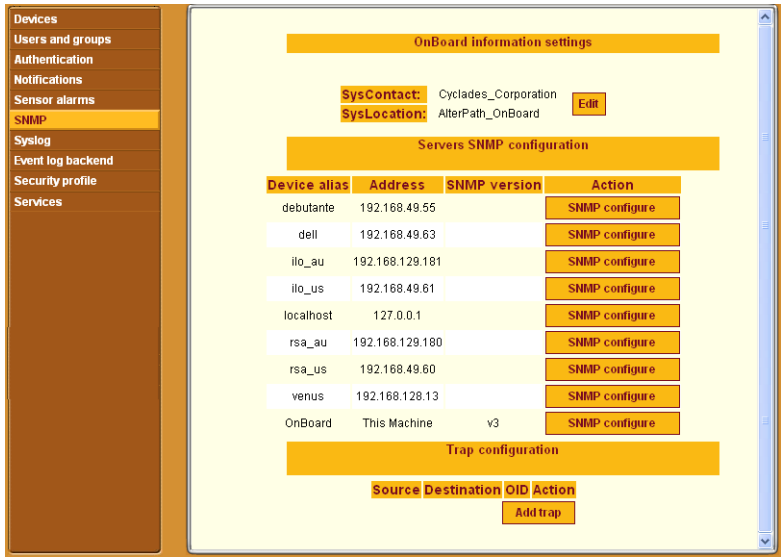


Figure 6-31: Config → SNMP Configuration Screen

Note: For SNMP to work you need to need to ensure that the selected security profile enables SNMP (by checking Config → Security profile screen) or that the SNMP service is active (by checking the Config → Services screen). (If the security profile in effect enables SNMP, you do not need to activate SNMP on the Services screen.)

The following table lists the tasks for configuring SNMP

Table 6-13: Tasks for Configuring SNMP

Task	Where Documented
Configure OnBoard contact and location information	“Configuring SNMP Information Settings” on page 211
Configure SNMP for devices	“Configuring SNMP for Devices” on page 212

Configuring SNMP Information Settings

Under the “OnBoard information settings” heading on the Config → SNMP screen shown in Figure 6-31, clicking the “Edit” button enables the administrative user to change the configured values. The “Edit” button brings up the screen shown in the following figure.

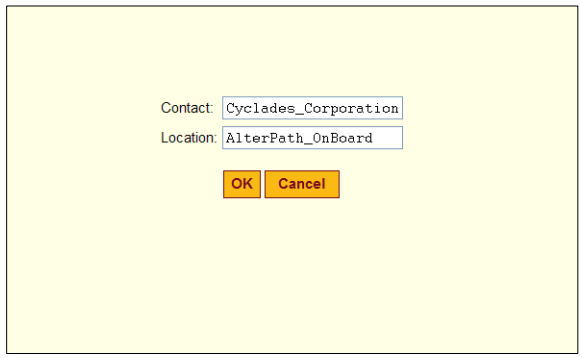


Figure 6-32: Config → SNMP: Edit OnBoard Information Settings

▼ To Configure OnBoard SNMP Information

1. Log into the Web Manager as an administrative user.
2. Go to Config → SNMP.
3. Click the “Edit” button next to the SysContact and SysLocation entries.
4. Accept or change the text in the “Contact” field.
5. Accept or change the location in the “Location” field.
6. Click OK.
7. Click “Save and apply changes.”

Configuring SNMP for Devices

Administrative users can use this screen to enable notifications about significant events occurring on connected devices to be sent from the OnBoard to an SNMP management application, such as HP Openview, Novell NMS, IBM NetView, or Sun Net Manager. As shown in Figure 6-33, the names of all configured devices that have service processors are listed under the "Servers SNMP configuration" heading on the Config → SNMP screen.

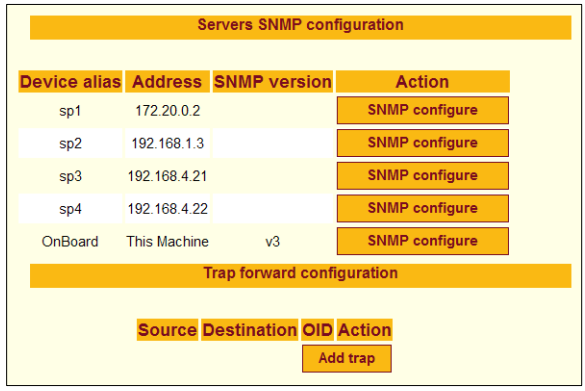


Figure 6-33: Config → SNMP: SNMP Configure Dialog

Pressing the "SNMP Configure" button next to the name of a device brings up the screen like the one shown in the following figure. The administrative user can use this screen to define the SNMP protocol for a device and configure SNMP access.

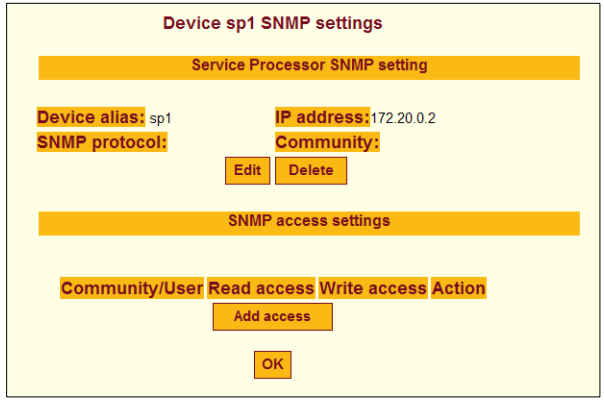


Figure 6-34: Device SNMP Settings Screen

Configuring Device SNMP Settings

When the administrative user clicks the “Edit” button under the “Service Processor SNMP setting” heading shown in Figure 6-34, a screen appears like the one shown in the following figure when “v1” is selected from the “SNMP version” menu.

Figure 6-35: Config → SNMP: Device SNMP Access Dialog With V1 Selected

When the administrative user clicks the “Edit” button under the “Service Processor SNMP setting” heading shown in Figure 6-33, a screen appears like the one shown in the following figure when “v2” is selected from the “SNMP version” menu.

Figure 6-36: Config → SNMP: Device SNMP Access Dialog With V2c Selected

When the administrative user clicks the "Edit" button under the "Service Processor SNMP setting" heading shown in Figure 6-33, a screen appears like the one shown in the following figure when "v2" is selected from the "SNMP version" menu.

Figure 6-37: Config → SNMP: Device SNMP Access Dialog With V3 Selected

Configuring SNMP Access Settings

When the administrative user clicks the “Add Access” button under the “Service Processor SNMP setting” heading shown in Figure 6-34, a screen appears like the one shown in the following figure.

Figure 6-38: Config → SNMP: Device SNMP Access Dialog With V1 Selected

The fields on the screen shown in Figure 6-38 vary according to which SNMP protocol type is selected. Figure 6-38 shows the fields when v1 is selected.

Figure 6-39 shows the fields when v2c is selected from the “SNMP version” menu.

Figure 6-39: Config → Device SNMP Settings Dialog With V2c Selected

Figure 6-40 shows the fields when v3 is selected from the “SNMP version” menu.

Figure 6-40: Config → Device SNMP Settings Dialog With V3 Selected

Fields and Menu Items for Configuring SNMP for Devices

The following table lists the fields for configuring SNMP for devices.

Table 6-14: Fields for Configuring SNMP

Field or Menu Name	Description
OID	Object Identifier. Each managed object has a unique identifier.
SNMP version	v1 v2c v3
Community	SNMP v1 and v2c only. The community name is sent in every communication between the client and the server, and the community name must be correct before requests are allowed. The most common community is “public,” and it should not be used because it is so commonly known. By default, the public community cannot access SNMP information on the OnBoard.
Fields for configuring SNMP v3 only:	
User name	Username used for authentication
Auth method	• MD5 • SHA

Table 6-14: Fields for Configuring SNMP (Continued)

Field or Menu Name	Description
Auth pass	Password used for authentication
Encryption	• DES • AES
Crypt pass	Password used for encryption

▼ *To Configure SNMP for a Device*

1. Log into the Web Manager as an administrative user.
2. Go to Config → SNMP.
3. Click the "SNMP configure" button for the desired device under the "Servers SNMP configuration" heading.

   The "Device *devicename* SNMP settings" dialog appears.
4. To configure the devices SNMP settings, do the following steps.
   a. Click "Edit" under the "Service Processor SNMP setting" heading.

      The "Device *devicename* SNMP settings" dialog appears.
   b. Enter the object identifier in the OID field.
   c. Select a version from the SNMP version pull-down menu.
   d. If either the v1 or v2c version is selected in Step c, enter a community name in the "Community field.
   e. If the v3 version is selected in Step c, do the following steps.
      i. Enter the user name required for authentication in the "User name" field.
      ii. Select an authentication method from the "Auth method" pull-down menu.
      iii. Enter the authentication password in the "Auth pass" field.
      iv. Select an encyrption method from the "Encryption" pull-down menu.

f. Enter the appropriate password for the encryption method in the "Crypt pass" field.

5. Click OK.

6. To configure SNMP access settings, do the following steps.

a. Click the "Add access" button under the "SNMP access settings" heading.

The "Device -*devicename*- SNMP access configuration" screen appears.

b. Select a version from the "SNMP version" pull-down menu.

c. If either the v1 or v2c version is selected in Step b, do the following steps.

i. Enter a community name in the "Community" field.

ii. Enter a Source IP address in the "Source" field.

iii. If an authentication method has been configured, select a "Read view" and "Write view" from the "Security level" pull-down menus.

d. If the v3 version is selected in Step b, do the following steps.

i. Configure users as desired by clicking the "Add user" button and filling out the fields and selecting from the menu items on the "User settings" dialog that appears, then clicking OK.

ii. Enter a community name in the "Community" field.

iii. Enter a Source IP address in the "Source" field.

iv. Select a username from the "User" pull-down menu.

v. Depending on which authentication and encryption methods have been configured, select the appropriate "Read view" and "Write view" options that are available on the pull-down menus under "Security level."

e. Configure views as desired by performing the following steps.

i. Click the "Edit views" button.

The "Views configuration" screen appears.

ii. To add a view, click the "Add View" button.

The “SNMP view settings” dialog appears.

iii. Enter the desired name in the “View name” field.

iv. Fill out as many entries as desired with an OID and Mask, and select the desired “Include” and “Exclude” options from the pull-down menu on the left of each entry.

v. Click OK.

f. Click OK.

7. Click OK.

8. Click “Save and apply changes.”

Configuring Logging of System Messages (Syslogs)

When an administrative user goes to Config → Syslog, the screen shown in the following figure appears.

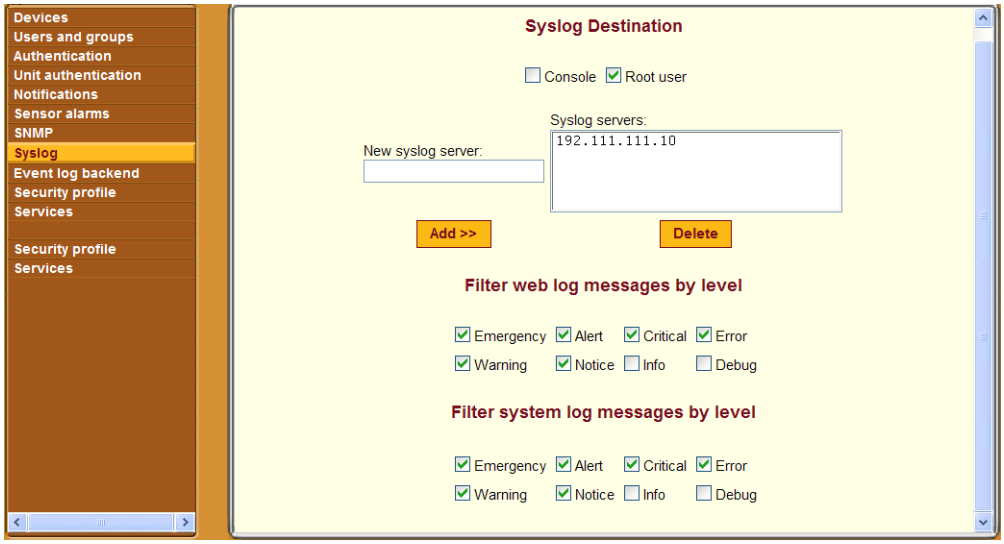


Figure 6-41: Config → Syslog Screen

An administrative user can use the Config → Syslog screen to do the following:

- Specify that syslog messages are sent to the console, to the root user, or to one or more syslog servers.
- Specify rules for filtering messages.

Syslog Destination

The administrative user can use the Config → Syslog screen to tell the OnBoard to send syslog messages to one or all of the following:

- Console
- Root user (if the root user is configured to receive syslog messages, make sure to configure an email address under Network -> Outbound email).
- Syslog server

Filter Messages by Level

The bottom of the Config → Syslog screen has two sets of checkboxes for specifying which types of web log and system log messages are forwarded based on their severity level:

- Emergency
- Alert
- Critical
- Error
- Warning,
- Notice
- Info
- Debug

▼ *To Configure the Syslog Destination and Message Filtering*

1. Go to Config → Syslog.

   The Syslog screen displays.

2. Select a destination for the Syslog messages by doing one or more of the following steps as desired.

   a. To configure messages to be sent to the console, click the “Console” checkbox.

   b. To configure messages to be sent to the root user, click the “Root user” checkbox.

   c. To configure messages to be sent to a syslog server, add a syslog server to the Syslog servers list by doing the following steps.

      i. Enter a syslog server’s IP address in the “New syslog server” field

      ii. Click the “Add>>” button.

      iii. To add additional syslog servers, repeat steps Step i and Step ii.

3. On the “Filter web log messages by level” screen, specify which types of web log messages are forwarded by clicking the checkboxes next to the desired severity levels.

4. On the “Filter system log messages by level” screen, specify which types of system log messages are forwarded by clicking the checkboxes next to the desired severity levels.

5. Click “Save and apply changes.”

Configuring the Event Log Backend

When an administrative user goes to Config → Event log backend, a screen appears like the one shown in the following figure. An entry appears for each configured device with an “Edit” button next to each device’s entry.

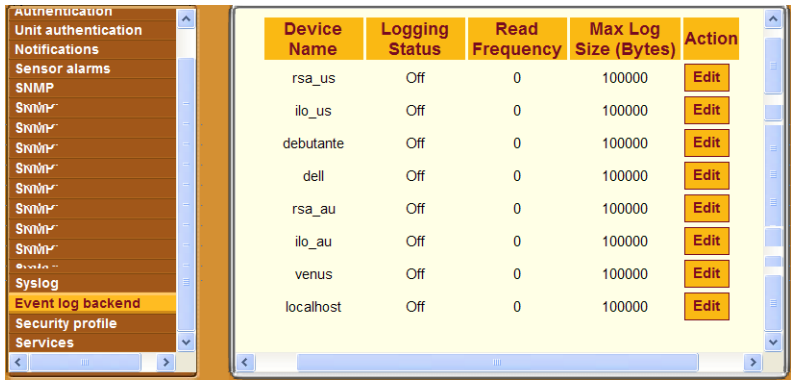


Figure 6-42: Config → Event Log Backend Screen

An administrative user can use the Config → Event log backend screen to configure event logging for connected service processors.

Clicking the “Edit” button on the Event log backend screen brings a dialog like the one shown in the following screen example.

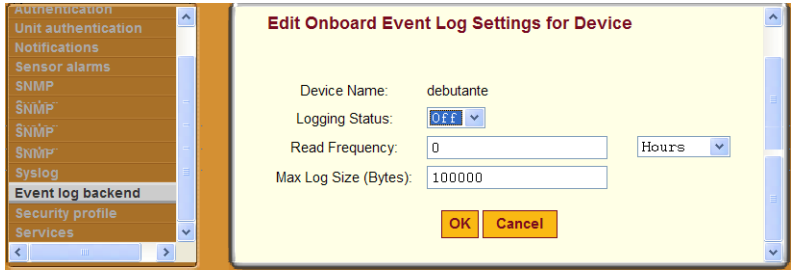


Figure 6-43: Config → Event Log Backend: Edit Dialog

▼ *To Configure Event Logging for Connected Service Processors*

1. Log into the Web Manager as an administrative user.
2. Go to Config → Event log backend.

   The Event log backend profile screen displays.
3. Click the “Edit” button to edit event logging for a device.

   The “Edit OnBoard Event Log Settings for Device” displays.
4. Select “On” or “Off” from the Logging Status pull-down menu or accept the currently-selected menu option.
5. Change or accept the number in the “Read Frequency” field, select “Hours” or “Minutes” from the pull-down menu, or accept the currently-selected menu option.
6. Change or accept the number of bytes in the “Max Log Size (Bytes)” field.
7. Click OK.
8. Click “Save and apply changes.”

Selecting or Configuring a Security Profile

When an administrative user goes to Config → Security profile, the screen shown in the following figure appears.

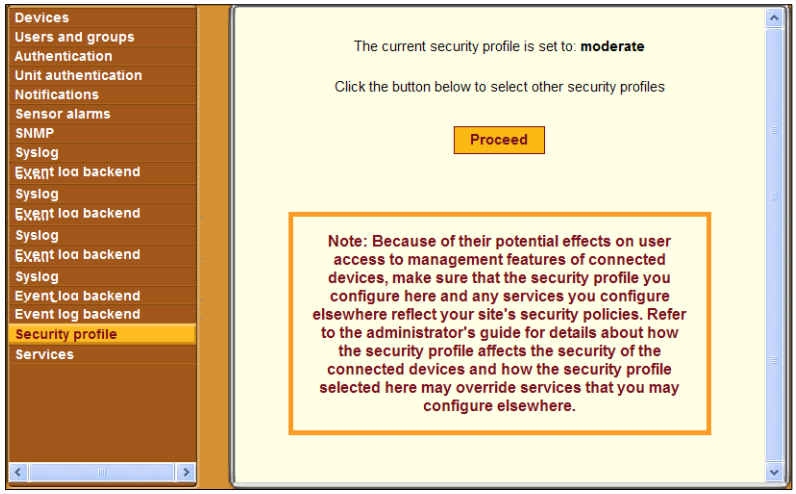


Figure 6-44: Config → Security Profile Screen

The note at the bottom of the security profile configuration screen is a reminder that putting another security profile into effect could disable or enable services that may have been turned on or off by some other means.

Clicking the “Proceed” button on the Security Profile Caution screen brings up the Security Profile configuration dialog shown in the following figure.

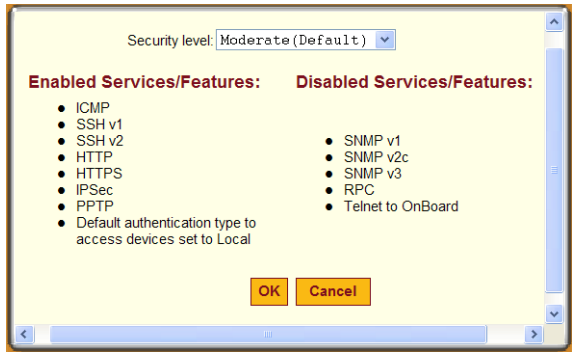


Figure 6-45: Config → Security Profile Dialog With the "Moderate" Profile Enabled

An administrative user can use the Config → Security profile screen to select one of the default security profiles or configure a custom security profile for the OnBoard. See "Understanding Security Profiles" on page 12 for important background information.

The features in the "Moderate" security profile are described in Table 1-6, "Moderate Security Profile Services/ Features," on page 12.

The Moderate profile is the default option selected on the "Security level" menu. The screens for the three other security profile are described in the following sections:

- "Secured" on page 226
- "Open" on page 227
- "Custom" on page 228

Secured

The following figure shows the lists of enabled and disabled features in the dialog for the “Secured” security profile.

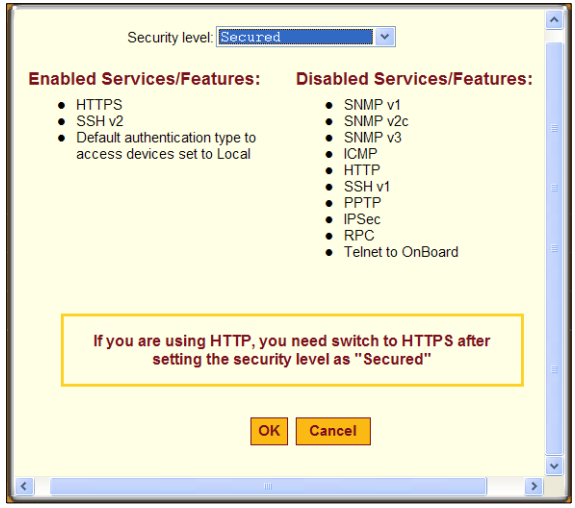


Figure 6-46: Config → Security Profile Dialog With the “Secured” Profile Enabled

---

Note: Follow the reminder at the bottom of the screen shown in Figure 6-46 by making sure to notify all users that they must use HTTPS when bringing up the Web Manager, because HTTP is disabled by the secured security profile.

The features in the “Secured” security profile are described in Table 1-7, “Secured Security Profile Services/Features,” on page 13.

Open

The following figure shows the lists of enabled and disabled features in the dialog for the “Open” security profile.

Figure 6-47: “Open” Security Profile Dialog

The features in the “Open” security profile are described in Table 1-8, “Open Security Profile Services/Features,” on page 13.

Custom

The following figure shows the features that can be enabled and disabled in the dialog for the “Custom” security profile.

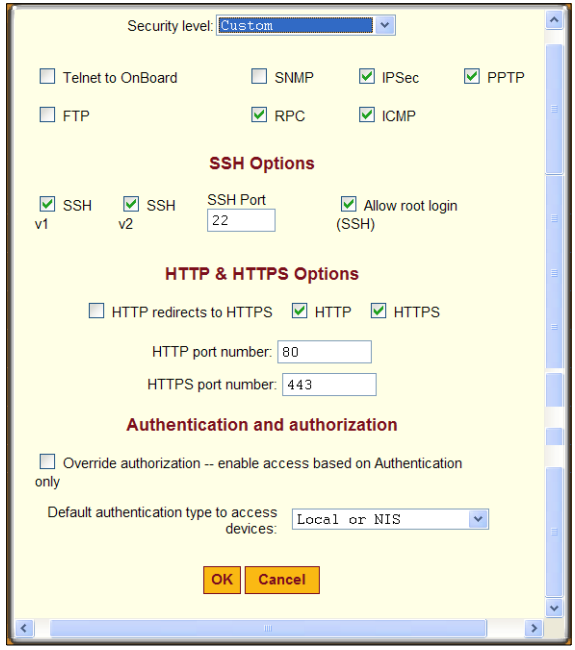


Figure 6-48: “Custom” Security Profile Dialog

The options that can be configured in a custom security profile are described in Table 1-9, “Services and Other Functions in the “Custom” Security Profile,” on page 14.

Note: Selecting a default authentication type means that the specified authentication type is selected by default in the Web Manager when a new device is being configured, and the default authentication type is assigned by default to a new device configured using the `cycli` utility after the security profile goes into effect. The administrative user can change the authentication type for each individual device while configuring it.

▼ *To Select the OnBoard's Security Profile*

1. Log into the Web Manager as an administrative user.
2. Go to Config → Security profile.

   The Security profile screen displays.
3. Click the "Proceed" button.
4. Select a security profile from the "Security Level" pull-down menu.
5. If you select the "Custom" profile, make sure the checkboxes are checked next to services and features you want to be enabled and make sure the checkboxes are clear next to services and features you want to be disabled.
6. Click "OK."

   The security profile confirmation screen appears.
7. Click the "Save and apply changes" button.

Configuring the OnBoard's Services

When an administrative user goes to Config → Services, the screen shown in the following figure appears. Checkmarks appear next to the services that have been enabled by default.

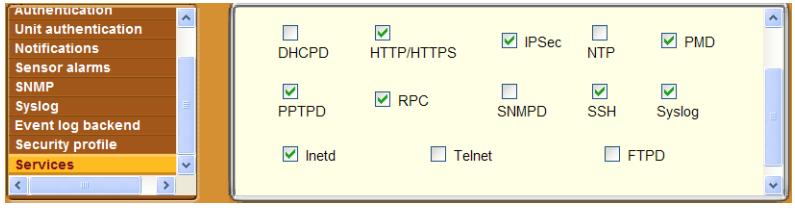


Figure 6-49: Config → Services Screen

An administrative user can use the Config → Services screen to enable or disable any of the listed network services. See "Understanding Services on the OnBoard" on page 17 for important background information.

▼ *To Configure Services*

1. Log into the Web Manager as an administrative user.
2. Go to Config → Services.

   The Services screen displays.
3. Click to check a checkbox next to each service you want to enable.
4. Click to leave unchecked any previously-enabled service that you want to disable.
5. Click "Save and apply changes."

Chapter 7
Web Manager “Network” Menu Options

This chapter describes the menu options available to administrative users under the “Network” top menu option.

For an overview of all the Web Manager features and menu options that are available for administrative users, see Chapter 2, “Web Manager Introduction,” if needed.

This chapter covers the topics in the following sections.

Options Under “Network”	Page 232
Configuring Network Interfaces	Page 233
Configuring Firewall Rules for OnBoard Packet Filtering	Page 239
Configuring Hosts	Page 242
Configuring Static Routes	Page 244
Configuring VPN Connections	Page 246
Configuring an Address for System Emails	Page 250
Configuring Private Subnets and Virtual Networks	Page 251

This chapter provides the procedures listed in the following table.

To Add a New Packet Filtering (Firewall) Rule	Page 241
To Add a New Host	Page 243
To Add a Static Route	Page 245
To Configure IPSec VPN	Page 247
To Configure a PPTP VPN Connection	Page 249
To Configure Outbound Email	Page 250

To Configure a Private Subnet	Page 254
To Configure a Virtual Network	Page 255

Options Under “Network”

When an administrative user clicks the “Network” option in the top menu of the Web Manager, seven options appear in the left menu, as shown in the following figure.

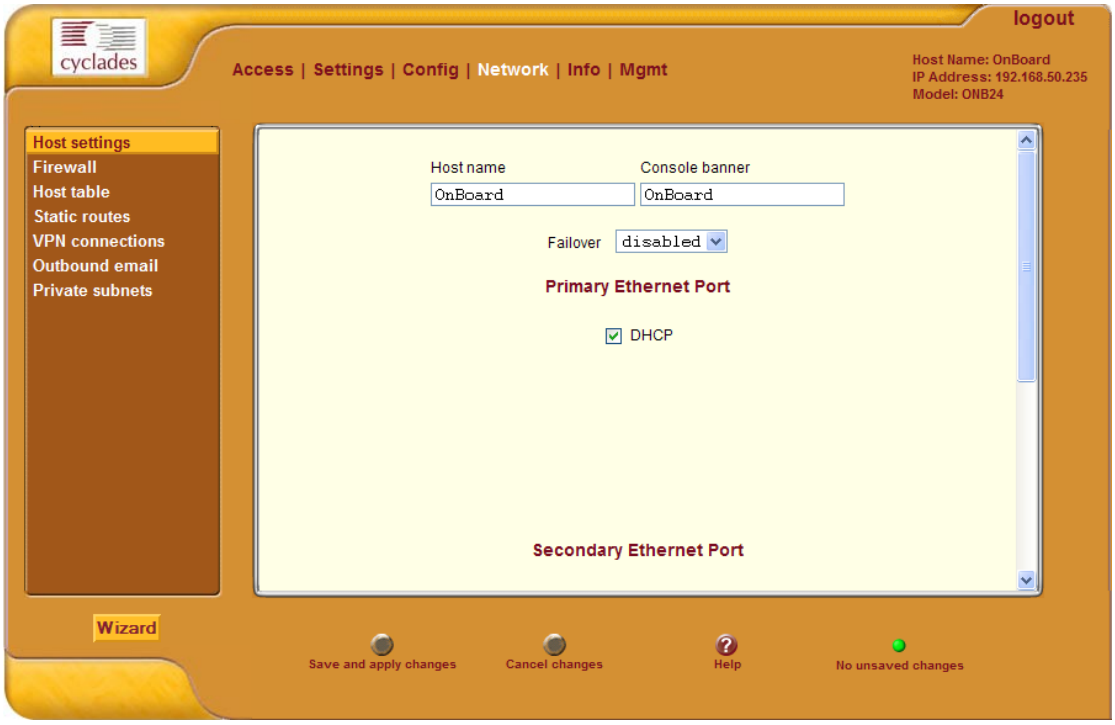


Figure 7-1: “Network” Menu Options

The options that appear when an administrative user clicks “Network” are described in the sections listed below.

Table 7-1: Options Under “Network”

Option	Where Described
Host Settings	“Configuring Network Interfaces” on page 233
Firewall	“Configuring Firewall Rules for OnBoard Packet Filtering” on page 239
Host table	“Configuring Hosts” on page 242
Static routes	“Configuring Static Routes” on page 244
VPN connection	“Configuring VPN Connections” on page 246
Outbound email	“Configuring an Address for System Emails” on page 250
Private subnets	“Configuring Private Subnets and Virtual Networks” on page 251

Configuring Network Interfaces

When an administrative user clicks the “Host settings” option under “Network,” a screen like the one shown in the following figure appears.

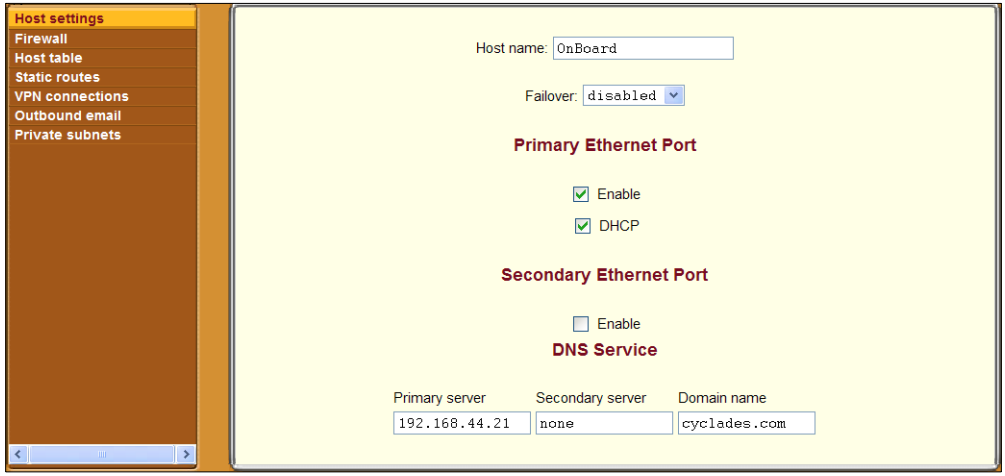


Figure 7-2: Network → Host Settings Screen

The administrative user can use this screen to configure the OnBoard's network interfaces. (For background information on configuring the Ethernet interfaces, see "Understanding Ethernet Ports on the OnBoard" on page 41.) The administrative user also can configure DNS for the OnBoard by entering the DNS server and domain name information at the bottom of the screen.

The screen shown in Figure 7-2 allows the administrative user to set or change the parameters in the following table.

Table 7-2: Network Interfaces Configuration Values

Settings	Notes
Failover	Selecting "enabled" from the pull-down menu configures failover from the primary to the secondary Ethernet port if the primary port goes down. See "Configuring Failover" on page 236.
	Selecting "disabled" causes additional fields to display to allow configuration of one or both of the public Ethernet ports. See "Configuring Primary and Secondary Ethernet Ports" on page 236.
Host name	Default: OnBoard
Primary DNS server	IP address for a primary DNS server on the same subnet as the OnBoard
Secondary DNS server	IP address for an optional secondary DNS server on the same subnet as the OnBoard
Domain name	Domain name used on the domain name server (DNS)

Keep following two issues in mind when configuring public Ethernet ports:

- When an interface is configured for DHCP and the DHCP server cannot be reached for any reason, the interface IP address falls back to the preconfigured default static IP address (192.168.160.10) unless an OnBoard administrator has assigned an IP address to the interface.
- When both interfaces are active and assigned two different IP addresses, both interfaces are reachable through either IP address even if the cable is disconnected from one of the interfaces.

Configuring Routes

Configuring the network interfaces sets up a default route for the OnBoard. When the DHCP checkbox is checked on any of the network interface screens, the DHCP server assigns the OnBoard a default route. If the DHCP checkbox is not checked, the gateway IP specified by the administrative user in the “Gateway IP” field is used to create a default route for the interface. If a host or network route is required, the administrative user should go to the Network → Static routes screen.

Configuring Failover

The following figure shows the fields that appear on the Network → Host Settings screen when the "enabled" option is selected from the Failover menu and the DHCP option is not checked. If the DHCP option is checked, no further configuration is needed.

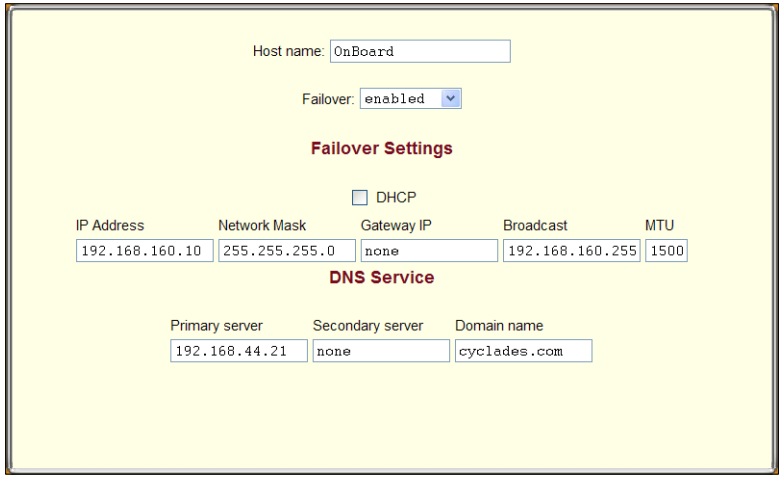


Figure 7-3: Network → Host Settings Screen With Failover Enabled

With failover enabled, the secondary Ethernet interface becomes bonded to the primary Ethernet interface, and the secondary Ethernet interface becomes active only if the primary Ethernet port is not available. As a result, the values entered in the fields on the screen shown in Figure 7-3 apply to the single bond0 interface.

Configuring Primary and Secondary Ethernet Ports

If failover is disabled, the administrative user can configure each Ethernet port separately in the following ways:

- Enable or disable each Ethernet port
- Enable or disable DHCP
- If DHCP is disabled, configure each port for static IP addressing.

The example in the following figure shows the fields that appear on the Network → Host Settings screen when both the primary and secondary

Ethernet ports are enabled and DHCP is disabled. The fields shown in Figure 7-4 are for the following purposes:

- Configuring basic network parameters and assigning a static IP address to the Ethernet port (s)
- Configuring DNS

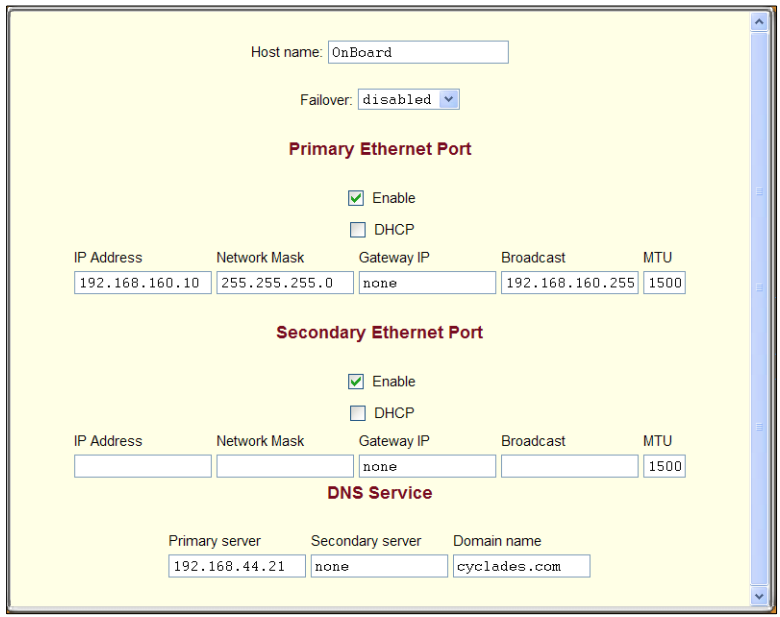


Figure 7-4: Network → Host Settings Screen With Both Interfaces Enabled and DHCP Disabled

▼ *To Configure OnBoard Network Interfaces*

1. Log into the Web Manager as an administrative user.

   See “To Log Into the Web Manager” on page 75, if needed.

2. Go to Network → Host settings.
3. Modify the name in the “Host name” field, if desired.
4. Enable or disable failover by selecting the desired option from the “Failover” pull-down menu.

5. Enable DHCP, if desired, by making sure the “DHCP” checkbox is checked.
6. Configure a static IP address, if desired, for an Ethernet port by performing the following steps.
   a. Disable DHCP by making sure the “DHCP” checkbox is not checked.
   b. Enter or modify the IP address in the “IP address” field.
   c. Enter or modify the netmask in the “Network Mask” field.
   d. Enter or modify the IP address for a network gateway in the “Gateway IP” field.

Note: The IP address entered in the “Gateway IP” field is used for the OnBoard’s default route.

---

   e. Enter or modify a broadcast IP address in the “Broadcast” field.
   f. Enter or modify the maximum transmission unit value for the Ethernet port in the “MTU” field.
7. Configure DNS, if desired, by performing the following steps.
   a. Enter or modify the IP address for the primary DNS server in the “Primary DNS” field.
   b. Enter or modify the IP address for an optional secondary DNS server in the “Secondary DNS” field.
   c. Enter or modify an existing domainname in the “Domain name” field.
8. Click “Save and apply changes.”

Configuring Firewall Rules for OnBoard Packet Filtering

When an administrative user clicks the “Firewall” option under “Network,” a screen appears like the one shown in the following figure. The administrative user can use this screen to configure packet filtering as described in this section. See “Understanding Firewall/Packet Filtering on the OnBoard” on page 63 for background information, if needed.

Figure 7-5: Network → Firewall Screen

The Network → Firewall screen provides an interface to `iptables`. Using this screen, the administrative user can define rules for the built-in chains. Once rules have been administratively-defined, they can be edited or deleted.

Figure 7-5 shows the six built-in chains. The rules for the built-in chains are hidden. The top three chains are defined in the `iptables` "filter" table and the bottom three chains are defined in the `iptables` "nat" table. Also as shown, an "Add new *table_name chain_name* rule" button appears under the entry for each chain, for example, "Add new NAT prerouting rule."

Administrative users may want to add rules to the default chains to suit their environment and their needs. The example in Figure 7-5 shows an example of an administratively-defined rule for the filter table INPUT chain. The number 0 is assigned automatically. As shown, an "Edit" and "Delete" button appear next to the entry for each administrator-defined rule.

The administrative user can use the "Edit," "Delete," and "Add new *table_name chainname* rule" buttons on the form to do the following:

- Add new rules
- Edit administrator-added rules
- Delete administrator-added rules

Adding a Rule

Clicking an "Add new *table_name chainname* rule" button brings up a dialog like the one shown in the following figure, which shows the dialog that appears when the administrative user clicks the "Add new NAT prerouting rule" button.

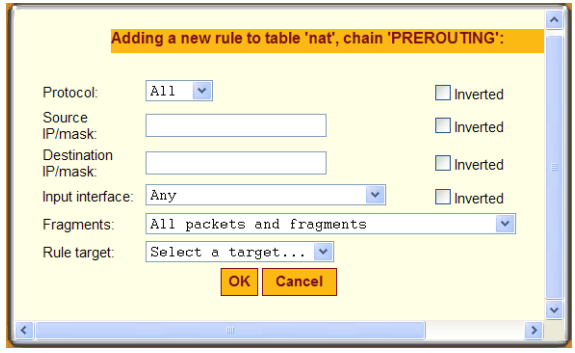


Figure 7-6: Network → Firewall: Add Rule Dialog

See Table 1-25, "Filter Options for Packet Filtering Rules," on page 65 for definitions of the filter options on the dialog shown in Figure 7-6.

▼ To Add a New Packet Filtering (Firewall) Rule

1. Log into the Web Manager as an administrative user.

   See “To Log Into the Web Manager” on page 75, if needed.

2. Go to Network → Firewall.
3. Click the “Add new *table_name chainname* rule” button underneath the entry for the chain to which you wish to add a rule.
4. Configure one or more of the following filtering options, as desired.
   a. Select a protocol from the “Protocol” pull-down menu.
   b. Specify a source IP and subnet mask in the form: *hostIPaddress or networkIPaddress/NN.*
   c. Specify a destination IP and subnet mask in the form: *hostIPaddress or networkIPaddress/NN.*
   d. Depending on which chain you selected, select an input or output interface from the “Input interface” or “Output interface” pull-down menu.
   e. Choose the types of packets to be filtered from the “Fragments” pull-down menu.
   f. Select a target from the “Rule target” pull-down menu.
5. Click OK.
6. Click the “Save and apply changes” button.

▼ To Edit an Administrator-added Packet Filtering (Firewall) Rule

1. Log into the Web Manager as an administrative user.

   See “To Log Into the Web Manager” on page 75, if needed.

2. Go to Network → Firewall.
3. Click the “Edit” button for the entry for the rule you want to change.
4. Configure one or more of the following filtering options, as desired.
   a. Select or accept the protocol selected from the “Protocol” pull-down menu.

b. Accept or change the value entered in the Source IP/mask field, using the form: *hostIPaddress* or *networkIPaddress/NN,* where *NN* is the subnet length.

c. Accept or change the value entered in the Destination IP/mask in the form: *hostIPaddress*r *networkIPaddress/NN,* where *NN* is the subnet length.

d. Depending on which type of chain is selected, accept or change either the input or output interface selected from the "Input interface" or "Output interface" pull-down menu.

e. Accept or change the types of packets to be filtered selected from the "Fragments" pull-down menu.

f. Accept or change the target selected from the "Rule target" pull-down menu.

5. Click OK.

6. Click the "Save and apply changes" button.

Configuring Hosts

When an administrative user clicks the "Host table" option under "Network," a screen like the one shown in the following figure appears.

Figure 7-7: Network → Host Table Screen

The administrative user can use the "Edit," "Delete," and "Add new host" buttons on the form to do the following:

- Add a new host
- Edit the host's configuration
- Delete host entries

The following figure shows the dialog that appears when the administrative user clicks the “Add new host” button on the screen shown in Figure 7-7.

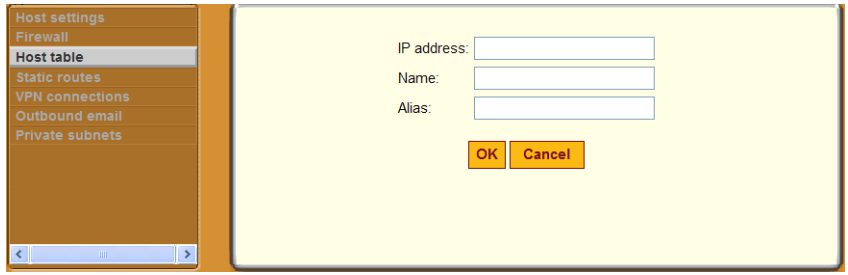


Figure 7-8: Network → Host Table: Add New Host Dialog

When adding a host, the administrative user must enter the information in the top two bullets below:

- IP address
- Name
- Alias

The “Alias” is optional

▼ *To Add a New Host*

1. Log into the Web Manager as an administrative user.

   See “To Log Into the Web Manager” on page 75, if needed.

2. Go to Network → Host table.
3. Enter an IP address in the “*IP address*” field.
4. Enter a hostname in the “Name” field.
5. Optionally, enter an alias for the host
6. Click OK.
7. Click the “Save and apply changes” button.

Configuring Static Routes

When an administrative user clicks the “Static routes” option under “Network,” a screen like the one shown in the following figure appears.

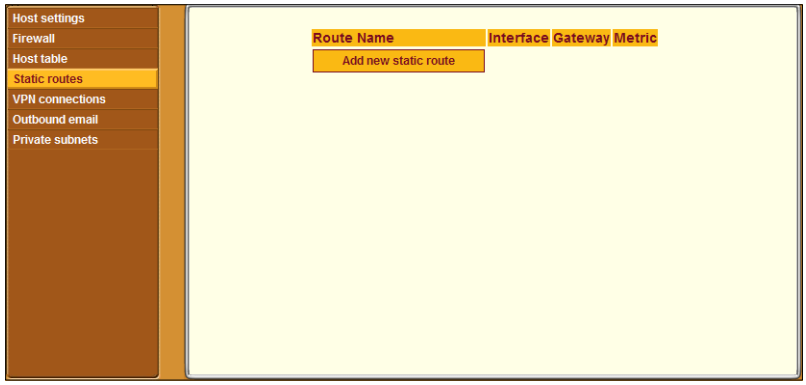


Figure 7-9: Network → Static Routes Screen

The administrative user can use the Static routes screen to manually add a static route or to edit or delete existing static routes.

Figure 7-10 shows the dialog that appears when the administrative user clicks the “Add new static route” button on the screen shown in Figure 7-9.

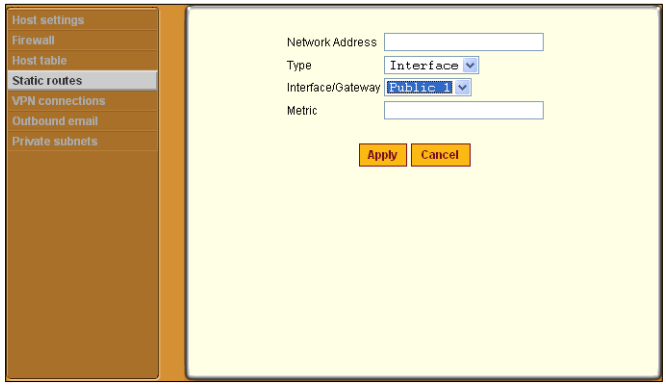


Figure 7-10: Network → Add New Static Route Dialog

The following table describes the fields and menu options that appear when you select the “Edit” or “Add” buttons.

Table 7-3: Fields and Menus for Configuring Static Routes

Field or Menu Name	Definition
Network Address	Enter the IP address of the destination host or specify a network in the form *networkIPaddress*/*mask_length* (also referred to as prefix/length). **Note:** To set a default route, go to Network → Host Settings.
Type	Pull-down menu choices are “Gateway” or “Interface.”
Interface/Gateway	• When “Interface” is selected from the “Type” menu, the “Interface/Gateway” menu choices are: •Public 1 •Public 2 •Failover •PCMCIA 1 •PCMCIA 2 • When “Gateway” is selected from the “Type” menu, a field appears for entering the IP address of the gateway.
Metric	Enter the number of hops to the destination.

▼ *To Add a Static Route*

1. Log into the Web Manager as an administrative user.

   See “To Log Into the Web Manager” on page 75, if needed.
2. Go to Network → Static routes.
3. Enter a network IP address in the “Network Address” field.
4. Select “Interface” or “Gateway” from the “Type” pull-down menu.
5. Enter the number of hops to the destination in the “Metric” field.
6. Click “Apply.”
7. Click the “Save and apply changes” button.

Configuring VPN Connections

An administrative user must configure VPN connections in order to enable authorized users to access native IP management features on an SP.

See the *AlterPath OnBoard User's Guide* for background information about how users create a VPN connection from their remote computers to enable access native IP features on an SP. Also see "Example 2: Two Private Subnets and VPN Configuration" on page 345.

The Web Manager Network → VPN connections screen appears as shown in the following figure.

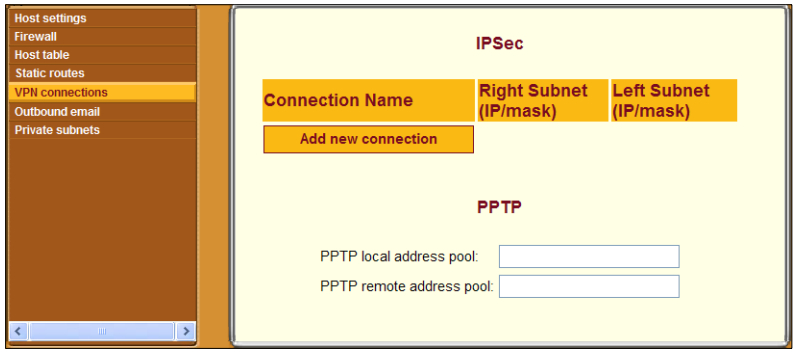


Figure 7-11: Network → VPN Connections Screen

The administrative user configures IPSec differently from PPTP connections, as described in the following subsections:

- "Configuring IPSec VPN Connections" on page 247
- "Configuring PPTP VPN Connections" on page 248

Configuring IPSec VPN Connections

Selecting “Add new connection” on the VPN connections screen under the IPSec heading brings up the screen shown in the following figure.

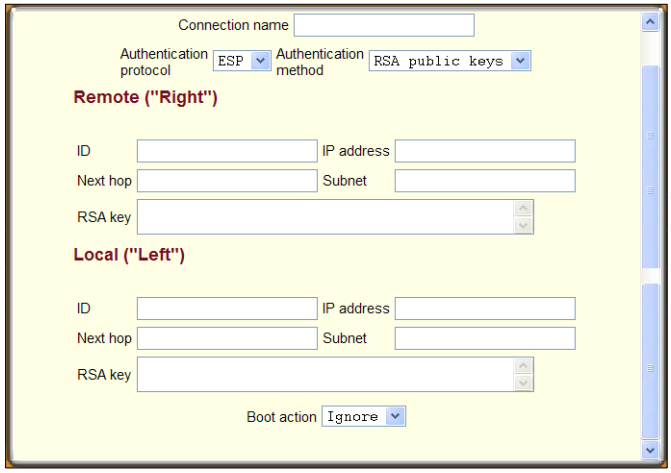


Figure 7-12: IPSec VPN Connection Configuration Dialog

The administrative user can define multiple IPSec VPN connections.

▼ *To Configure IPSec VPN*

Make sure that the IPsec service is enabled. See Table 1-16, “IPSec VPN Configuration Information for Administrators and Users,” on page 35, if needed, for details about the values to enter.

1. Log into the Web Manager as an administrative user.

   See “To Log Into the Web Manager” on page 75, if needed.

2. Go to Network → VPN connections.

   The VPN connections screen appears.

3. Click “Add new connection.”

4. IPSec VPN Connection Configuration dialog appears

5. Enter any descriptive name you choose for the connection in the “Connection name” field.

6. Select either ESP or “AH” from the “Authentication protocol” pull-down menu.
7. Select “Shared Secret” or “RSA public keys” from the “Authentication method” pull-down menu.
8. If “Shared secret” is selected, enter the shared secret in the “Pre-Shared key” field.
9. Set up the right and left hosts by doing the following steps.
   a. Enter the name of the OnBoard (left host) or the remote computer (right host) in the “ID” field.
   b. Enter the IP address of the OnBoard (left host) or the remote computer (right host) in the “IP Address” field.
   c. Enter the IP address of the router through which the host’s packets reach the Internet in the “NextHop” field.
   d. Enter the netmask for the subnet in the “Subnet Mask” field.
10. If “RSA public keys” is selected in Step 7, do one of the following steps.
    a. When configuring the left host, generate the key for the OnBoard and use copy and paste to enter the key in the “RSA key” field.
    b. When configuring the right host, find out the key from the remote gateway (where the right host resides) and enter the key in the “RSA key” field.
11. Select either “Ignore, “Add,” or “Start” from the “Boot Action pull-down menu.
12. Click OK.
13. Click “Save and apply changes.”

Configuring PPTP VPN Connections

The OnBoard administrator can define a single PPTP VPN connection with a pool of IP addresses.

To configure the addresses used for all PPTP VPN connections between users and the OnBoard, the administrative user needs to fill in the PPTP fields shown in the following figure from the Network → VPN Connections Screen.

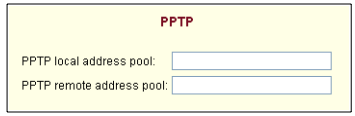


Figure 7-13: PPTP VPN Connection Configuration Fields

The following table describes the fields for configuring a PPTP profile. Specify a pool of addresses in the form 10.0.0.100-110.

Table 7-4: Fields for Configuring a PPTP Profile

Field	Purpose
PPTP local address pool	Assign an OnBoard IP address or range of addresses to be used whenever a user creates a PPTP VPN connection to the OnBoard.
PPTP remote address pool	Assign a remote IP address or range of addresses to be used whenever a user creates a PPTP VPN connection to the OnBoard.

If configuring a PPTP VPN connection, the administrative user also must ensure that users who are authorized for native IP are also authorized for PPTP connections.

▼ *To Configure a PPTP VPN Connection*

1. Log into the Web Manager as an administrative user.

   See “To Log Into the Web Manager” on page 75, if needed.

2. Got to Network → VPN connections.
3. Enter a single IP address or a pool of IP addresses in the “PPP local address pool” field.
4. Enter a single IP address or a pool of IP addresses in the “PPP remote address pool” field.
5. Click “Save and apply changes.”

6. Make sure that users who are authorized for native IP are also authorized for PPTP connections.

Configuring an Address for System Emails

An administrative user must specify an SMTP server and an email address for an administrator to receive email from the system, such as those generated by the cron daemon.

The Web Manager Network → Outbound email screen appears as shown in the following figure.

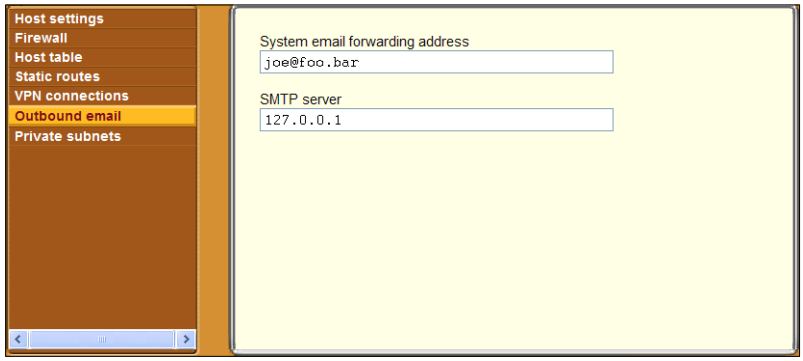


Figure 7-14: Network → Outbound Email Screen

▼ *To Configure Outbound Email*

1. Log into the Web Manager as an administrative user.

   See “To Log Into the Web Manager” on page 75, if needed.

2. Go to Network → Outbound email.
3. Enter an email address for an administrator to receive email from the system in the “System email forwarding address.”
4. Enter the DNS name or IP address for an SMTP server.
5. Click the “Save and apply changes” button.

Configuring Private Subnets and Virtual Networks

The administrative user performs configuration on the Network → Private subnets screen after deciding which addressing scheme to use, as discussed here and in more detail in Appendix , ‘Advanced Device Configuration” on page 309.” For introductory information, see also “Understanding Device Configuration” on page 53.

The Web Manager Network → Private subnets screen appears as shown in the following figure.

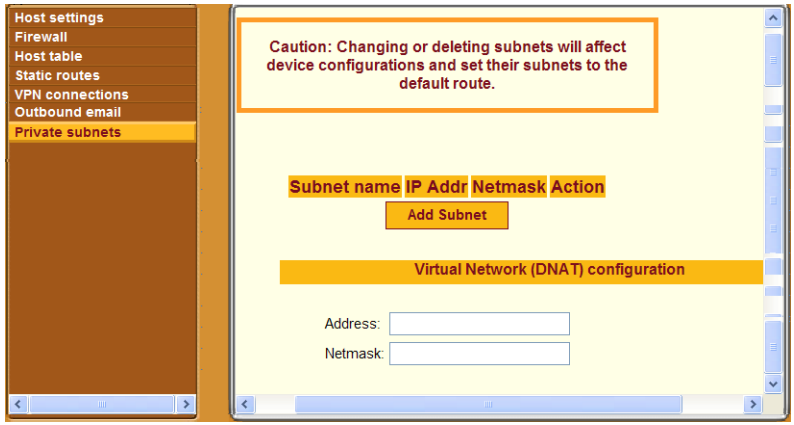


Figure 7-15: Network → Private Subnets Screen

The administrator must define at least one subnet, as described under “Adding Private Subnets” on page 251.

In certain cases, he administrator may also need to define a virtual Destination Network Address Translation (DNAT) network, as described under “Configuring a Virtual Network (DNAT)” on page 253.

Adding Private Subnets

The administrator must define at least one subnet to enable devices that are connected to the OnBoard’s private Ethernet ports to communicate on the Internet via the OnBoard’s public IP address. Any number of private subnets may be configured.

Note: The OnBoard attempts to reach a device that does not have a private subnet assigned by attempting to contact it through the OnBoard's default route. Therefore, unless the OnBoard administrator defines a public subnet and assigns it to each device, the device cannot be reached unless the device is on the public side of the OnBoard. In almost all cases, devices are on the private side of the OnBoard and therefore they are unreachable without a private subnet.

When an administrative user clicks the "Add Subnet" button on the Network → Private Subnets Screen, the "Private Subnet configuration" dialog appears, as shown in the following screen example.

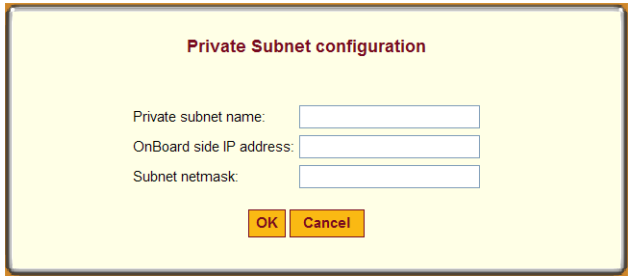


Figure 7-16: Network → Private Subnets: Add Subnet Dialog

A subnet is defined by configuring the following:

Table 7-5: Fields on the Private Subnet Configuration Dialog

Field	Definition
Private subnet name	Any meaningful name chosen by the administrator.
OnBoard side IP address	Devices use this address when communicating with the OnBoard. The OnBoard uses this address when communicating with devices. This address must be within the private subnet's IP address range)
Subnet mask	Used to define the range of addresses available on the subnet

The OnBoard derives the range of addresses in the subnet from the OnBoard-side IP address and the subnet mask. The OnBoard uses the specified information to create a route to the subnet in the OnBoard's routing table.

The example in Figure 7-17 shows a private subnet name of “net1,” an OnBoard side IP address of 192.168.0.254, and a subnet netmask of 255.255.255.0.

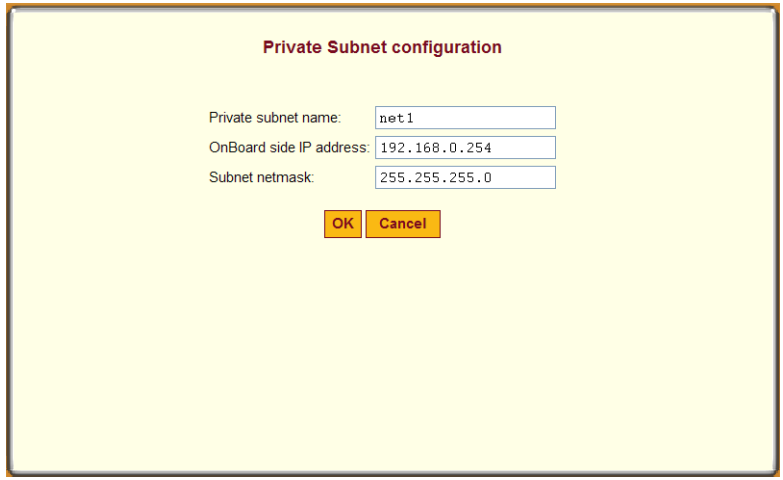


Figure 7-17: Network → Private Subnets: Add Subnet Dialog

The example in Figure 7-17 shows a private subnet name of “net1,” an OnBoard side IP address of 192.168.0.254, and a subnet netmask of 255.255.255.0. The private subnet address derived from this configuration is 192.168.0.0. Since the broadcast address is 192.168.0.255 (by convention) and the OnBoard’s address is 192.168.0.254, the administrator can assign an address between 192.168.0.1 and 192.168.0.253 when configuring a connected device.

Configuring a Virtual Network (DNAT)

The administrator must also define a virtual network based on Destination Network Address Translation (DNAT) in the following cases:

- When multiple *subnets* must be supported (as when connected devices are already configured using IP addresses from multiple address ranges and it is not feasible to change the already-defined device IP addresses)
- When one or more subnets is defined, and it is important to hide the addresses of the connected devices from users by the use of *virtual IP addresses*

The fields under “Virtual Network (DNAT) configuration” on the Network → Private Subnets screen appear as shown in the following screen example.

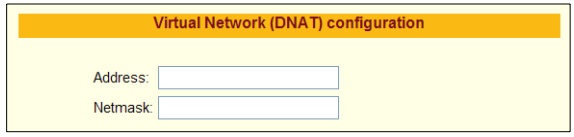


Figure 7-18: Network → Private Subnets: Virtual Network Configuration Fields

Table 7-6: Fields on the Private Subnet Virtual Network Configuration Dialog

Field	Description
Address	IP address to assign to the OnBoard from the virtual network’s address range. For example, if the virtual IP address of the network is 10.0.0.0, 10.0.0.254 would a valid IP address for the OnBoard that could be entered here.
Netmask	Netmask (which is used in combination with the network address portion of the “Address” above to define the address range of the virtual network.

▼ *To Configure a Private Subnet*

1. Log into the Web Manager as an administrative user.

   See “To Log Into the Web Manager” on page 75, if needed.

2. Click the “Add Subnet” button.

   The “Private Subnet configuration” dialog appears.

3. Enter a meaningful name for the private subnet in the “Private subnet name” field.
4. Enter an IP address for the OnBoard within the private subnet’s network address range in the “Onboard side IP address” field.
5. Enter a netmask for the private subnet in the “Subnet netmask” field.
6. Click OK.
7. Click “Save and apply changes.”

▼ *To Configure a Virtual Network*

1. Log into the Web Manager as an administrative user.

   See “To Log Into the Web Manager” on page 75, if needed.

2. Under “Virtual Network (DNAT) configuration,” enter a virtual IP address to assign to the OnBoard from the virtual network’s address range in the “Address” field.
3. Enter the netmask for the virtual network in the “Netmask” field.
4. Click OK.
5. Click “Save and apply changes.”

Chapter 8
Web Manager “Info” and “Mgmt” Menu Options

This chapter describes the menu options available to administrative users under the “Info” and “Mgmt” top menu options. For an overview of all the Web Manager features and menu options that are available for administrative users, see Chapter 2, “Web Manager Introduction,” if needed.

This chapter covers the topics in the following sections.

Options Under “Info”	Page 258
Viewing System Information	Page 259
Viewing System Information	Page 260
Viewing Information About Detected Devices	Page 263
Options Under “Mgmt”	Page 265
Backing Up or Restoring Configuration Files	Page 266
Upgrading OnBoard Firmware (Operating System Kernel, Configuration Files, and Applications)	Page 267
Restarting the OnBoard	Page 274

This chapter provides the procedures listed in the following table.

To Back Up Configuration Files	Page 267
To Restore Backed-up Configuration Files	Page 267
To Upgrade the OnBoard’s Operating System, Applications, and Configuration Files	Page 272
To Restart the OnBoard	Page 274

Options Under “Info”

When an administrative user clicks the “Info” option in the top menu of the Web Manager, three options appear in the left menu, as shown in the following figure.

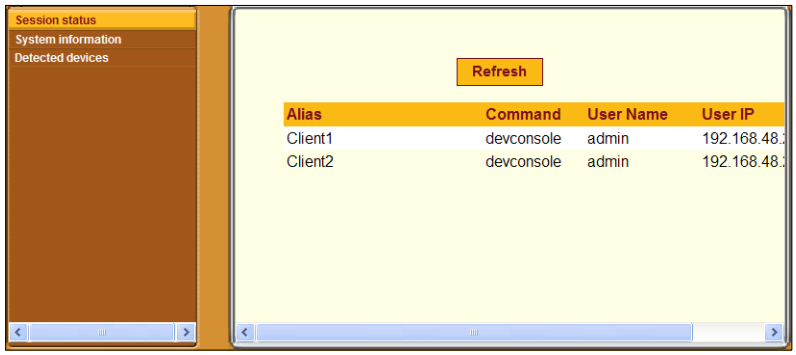


Figure 8-1: “Info” Menu Options

The options that appear when an administrative user clicks “Info” are described in the sections listed below.

Table 8-1: Options Under Info

Option	Where Described
Session status	“Viewing Status Information About Active Sessions” on page 259
System Information	“Viewing System Information” on page 260
Detected devices	“Viewing Information About Detected Devices” on page 263

Viewing Status Information About Active Sessions

When an administrative user goes to Info → Session status, a screen appears like the one shown in the following figure.

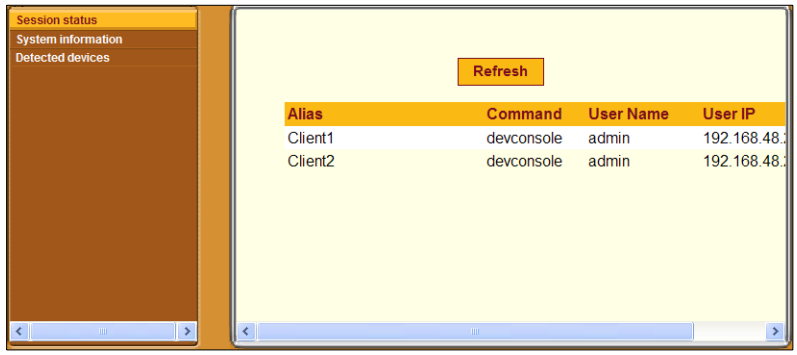


Figure 8-2: Info → Session Status Screen

The following table lists the headings on the Info → Session status screen.

Table 8-2: Information on the Info → Session Status Screen

Heading Name	Description
Alias	Name/alias configured for the device on the OnBoard
Command	Device management command being used
User Name	Name of the user account accessing the device
Port	Number of the OnBoard private port through which the device is being detected

Note: More than one device may be accessed through a single OnBoard private port; for that reason, configuration is done on devices not on ports. This screen is the only place where the port to which a device is connected is identified.

Viewing System Information

When an administrative user goes to Info → System information, a screen appears like the one shown in the following figure.

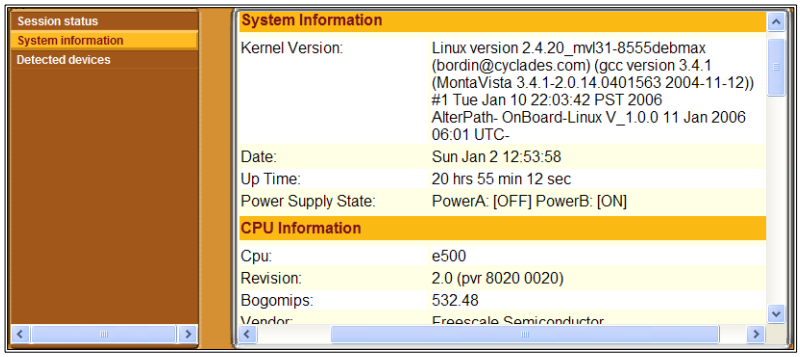


Figure 8-3: Info → System Information Screen

The following table lists the types of information available on the system information screen.

Table 8-3: Information on the System Information Screen

Heading	Listed Information
System Information	Kernel Version
	Date
	Up Time
	Power Supply State
CPU Information	CPU
	Revision
	Bogomips
	Vendor
	Machine
	Bus Frequency
	PVR
	SVR
	PLL Setting
	Memory

Table 8-3: Information on the System Information Screen (Continued)

Heading	Listed Information
Memory Information	MemTotal
	MemFree
	MemShared
	Buffers
	Cached
	SwapCached
	Active
	InActive
	HighTotal
	HighFree
	LowTotal
	LowFree
	SwapTotal
	SwapFree
	Committed_AS
	VmallocTotal
	VmallocUsed
	VmallocChunk
PCMCIA Information	Socket 0 – Ident[ity]
	Socket 0 – Config
	Socket 0 – Status
	Socket 1 – Ident[ity]
	Socket 1 – Config
	Socket 1 – Status

Table 8-3: Information on the System Information Screen (Continued)

Heading	Listed Information
RAM Disk Usage	Lists the partitions under the following headings Filesystem | 1k-blocks | Used | Available | Use% | Mounted

Viewing Information About Detected Devices

When an administrative user goes to Info → Detected devices, a screen appears like the one shown in the following figure.

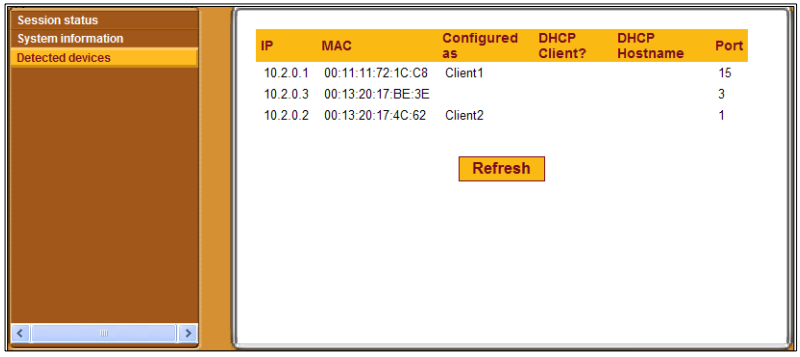


Figure 8-4: Info → Detected Devices Screen

The following table describes the information provided on the Info → Detected devices screen.

Table 8-4: Information on the Info → Detected Devices Screen

Heading Name	Description
IP	IP address of the detected device
MAC	MAC address of the detected device
Configured as	Name/alias configured for the device on the OnBoard

Table 8-4: Information on the Info → Detected Devices Screen (Continued)

Heading Name	Description
DHCP Client?	If the OnBoard DHCP server is enabled (as described in “Configuring the DHCP Server” on page 26) and if the detected device is running DHCP client software, YES appears in this column. In all other cases, the column is empty.
DHCP Hostname	If a DHCP server is enabled (as described in “Configuring the DHCP Server” on page 26), the OnBoard administrator usually assigns a fixed IP address along with a DHCP hostname to devices that have DHCP clients enabled. The DHCP hostname displays here.
Port	The number of the OnBoard private port through which the device is being detected.

Options Under “Mgmt”

Clicking the “Mgmt” (Management) option brings up the left menu options shown in the following screen example.

Figure 8-5: “Mgmt” Options

The following table describes the Menu Options under “Mgmt” and provides links to procedures.

Table 8-5: Tasks Performed Under the Web Manager “Mgmt” Tab

Task	Option	Where Documented
Backup or restore configuration files to flash or server	Backup / restore	“Backing Up or Restoring Configuration Files” on page 266

Table 8-5: Tasks Performed Under the Web Manager “Mgmt” Tab (Continued)

Task	Option	Where Documented
Upgrade the OnBoard’s operating system, applications from an ftp server	Firmware upgrade	“Upgrading OnBoard Firmware (Operating System Kernel, Configuration Files, and Applications)” on page 267
Restart (reboot) the OnBoard	Restart	“Restarting the OnBoard” on page 274

Backing Up or Restoring Configuration Files

When an administrative user goes to Mgmt → Backup/restore, the screen shown in the following figure.

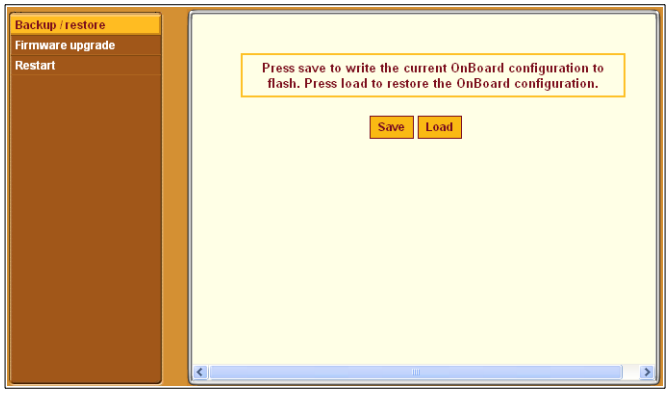


Figure 8-6: Mgmt → Backup/Restore Screen

Clicking the “Save” button backs up the current state of the Onboard configuration files in a single compressed backup file in flash memory and overwrites any previous backup file.

Clicking the “Load” button overwrites the current state of the configuration files with the last backup copy that was made.

See “Understanding How Configuration Changes Are Handled” on page 67, if needed, for more information.

▼ To Back Up Configuration Files

1. Bring up the Web Manager and log in.

   See “To Log Into the Web Manager” on page 75, if needed.

2. Go to Mgmt → Backup/restore.
3. Click the “Save” button to back up the current state of the configuration files.
4. Click the “Save and apply changes” button.

▼ To Restore Backed-up Configuration Files

1. Bring up the Web Manager and log in.

   See “To Log Into the Web Manager” on page 75, if needed.

2. Go to Mgmt → Backup/restore.
3. Click the “Restore” button to restore any previously-saved configuration files.
4. Click the “Save and apply changes” button.

Upgrading OnBoard Firmware (Operating System Kernel, Configuration Files, and Applications)

When an administrative user goes to the Mgmt → Firmware upgrade screen, the screen shown in the following figure appears.

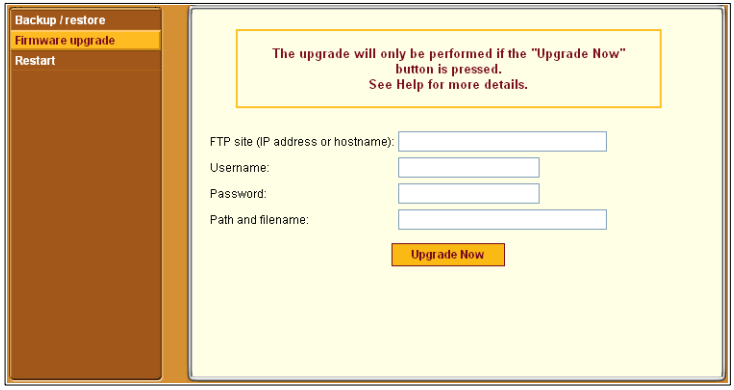


Figure 8-7: Mgmt → Firmware Upgrade Screen

An administrative user can use the screen to upgrade the OnBoard’s operating system kernel and applications, which are collectively referred to as “firmware” in Cyclades management interfaces.

Information Needed for Firmware Upgrades

The screen collects information used to automatically download software from an FTP server and to install the software on the OnBoard. The following table defines the information you need to supply on the form.

Table 8-6: Firmware Upgrade Screen Fields

Field/Menu Name	Definition
FTP site	The address of the FTP server where the firmware is located. You can use any ftp server if you download the firmware onto it first. The Cyclades ftp site address is: `ftp.cyclades.com`. See “To Download OnBoard Firmware From Cyclades” on page 269 for how to download the firmware for upgrading from a local ftp server.
Username	Username recognized by the ftp server. The Cyclades ftp username for firmware downloads is “anonymous.”
Password	Password associated with the username. An empty password is accepted for anonymous login at the Cyclades ftp server.
Image file (path and filename)	The pathname of the software image file on the ftp server. On the Cyclades ftp server, the directory is under /`pub/cyclades/alterpath/onboard/released/`*`version_number`*`/zImage_onb_`*`NNN`*, where *`version_number`* is `V_`*`N.N.N.`*, and *`N.N.N`* and *`NNN`* are the most recent version number, for example, `1.0.1` and `101`. Go to `ftp://ftp.cyclades.com/pub/cyclades/alterpath/onboard/released` in a browser, if needed, to verify the correct pathname and file names for the software for the OnBoard.

Configuration Backups Before Upgrading Firmware

Any configuration changes made after the last backup copy was made are lost unless the configuration files were backed up before the upgrade and then restored afterwards (see “Backing Up Configuration File Changes” on page 68 and “Restoring Backed Up Configuration Files” on page 69).

▼ *To Download OnBoard Firmware From Cyclades*

An administrator can use this procedure to download OnBoard firmware from the Cyclades ftp server onto a local ftp server.

After downloading the software onto the OnBoard by following this procedure, the administrative user needs to perform the procedure under “To Upgrade the OnBoard’s Operating System, Applications, and Configuration Files” on page 272 to upgrade the firmware.

1. Log into a local ftp server as root.
2. Change to the directory into which the software needs to be downloaded.

```
# cd /tmp
```

3. Enter the `ftp` command to access `ftp.cyclades.com`.

```
# ftp ftp.cyclades.com
Connected to ftp.cyclades.com (64.186.161.16).
220 “Welcome to Cyclades FTP service.”
Name (ftp.cyclades.com:root):
```

4. Enter “anonymous” when prompted for the “Name” and press “Enter” when prompted for the password.

```
Name (ftp.cyclades.com:admin): anonymous
331 Please specify the password.
Password: <Enter>
ftp>
```

5. Change directories to `/pub/cyclades/alterpath/onboard/released` and list the directories it contains.

```
ftp> cd /pub/cyclades/alterpath/pm/released
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    2 1006     100          4096 Sep 06  2006 V_1.0.0
drwxr-xr-x    2 1006     100          4096 Sep 06  2006 V_1.1.0
226 Directory send OK.
ftp>
```

As shown in the previous screen example, the directories are named for the software release numbers. The latest version in the example is `V_1.1.0`. If the latest version at the Cyclades site is more recent that the version installed on OnBoard, continue with this procedure to download the latest version.

6. Change directories to the directory with the highest (latest) version number and change to binary mode.

```
ftp> cd V_1.1.0
226 Directory send OK.
ftp> ls
150 Here comes the directory listing.
-rw-r--r--    1 1006     100        13611356 Jun 06 01:08 zImage_onb_110.bin
-rw-r--r--    1 1006     100        13611356 Jun 06 01:08 zImage_onb_110.md5
226 Directory send OK.
ftp> binary
200 Switching to Binary mode.
```

As shown in the previous screen example, the directory contains a binary file (`zImage_onb_`*version_number*`.bin`) for the latest software version, and a checksum file (`Image_onb_`*version_number*`.md5`).

7. Use the `mget` command to get the binary and md5 files (for example: `zImage_onb_110.bin`).

```
ftp> mget zImage_*
200 Switching to Binary mode.
mget ZImage_onb_100.bin? y
. . .
mget zImage_onb_110.md5? y
```

8. After the download completes, end the `ftp` connection, and verify the presence of the `zImage_onb_110.bin` and `zImage_onb_110.md5` files on the local server.

```
ftp> bye
221 Goodbye.
# ls
zImage_onb_110.bin
zImage_onb_110.md5
```

9. Log out from the console session and got to “To Upgrade the OnBoard’s Operating System, Applications, and Configuration Files.”

Special Considerations if the Last Boot Was a Network Boot

If the OnBoard was last booted over the network from a TFTP server, the message shown in the following figure appears.

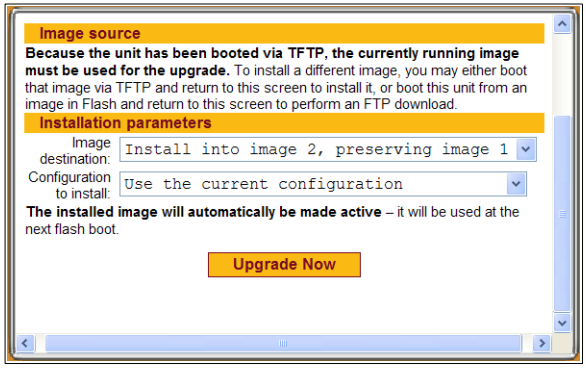


Figure 8-8: Mgmt → Firmware Upgrade Screen With Net Boot Message

If the last boot was a network boot from a TFTP server, clicking the “Upgrade Now” button writes the currently-running image from the RAM memory into the flash memory.

As described in a note on the screen shown in Figure 8-8, if the screen appears, the administrative user has two additional choices:

- Configure another image that resides on a TFTP server as the boot file, boot from the new image, and then return to this screen to upgrade the new image from the RAM memory.
- Boot from another image that is stored in the flash memory, and then use the current screen to download a new image using FTP.

The “Image destination” pull-down menu provides the following three choices:

- Install into image 1, preserving image 2
- Install into image 2, preserving image 1
- Erase Flash and install into image 1

The “Configuration to install” menu provides the following two choices:

- Use the current configuration
- Restore the factory default configuration

For more details about how images are stored in the OnBoard and about configuration file backups, see Appendix , ‘Advanced Boot and Backup Configuration Information” on page 371.

▼ *To Upgrade the OnBoard’s Operating System, Applications, and Configuration Files*

See Table 8-6, “Firmware Upgrade Screen Fields,” on page 268 if needed for the values to supply in the fields.

1. Log into the Web Manager as an administrative user.

   See “To Log Into the Web Manager” on page 75, if needed.

2. Go to Mgmt → Firmware upgrade.

3. To upgrade using an image from an TFTP server, do the following steps.

   a. Go to the Settings → Boot Configuration screen.

b. Specify the location of an image that resides on a TFTP server.

See “To Configure OnBoard Boot” on page 155 if needed.

c. Go to Step 4.

4. If the OnBoard is currently running an image from RAMDISK after a network boot and you want to write the image into the flash memory, do the following steps.

a. Select a destination for the image from the “Image destination” pull-down menu.

b. Choose whether to use the current configuration or the factory-default configuration from the “Configuration to install” menu.

c. Click the “Upgrade Now” button.

5. To upgrade using an image from an ftp server, do the following steps:

a. Enter the IP address or DNS name of the ftp server in the “FTP site” field.

b. Enter the username for the ftp site in the “Username” field.

c. Enter the password required for accessing the ftp site in the “Password” field.

d. Enter the pathname of the software image file on the ftp server in the “Image file” field.

e. Click the “Upgrade Now” button.

6. When the download completes, go to Mgmt → Restart and restart the OnBoard.

7. If you want to restore the configuration from the last backed-up copy, perform the following steps:

a. Go to the Mgmt → Backup/restore screen.

b. Click the “Load” button.

Note: Configuration file changes are maintained in RAMDISK until saved. Saved configuration file changes are applied to the new image after an upgrade. If you do not load a backed-up copy of the configuration files after the upgrade, the new software runs with the configuration files that were last saved before the upgrade was done.

Restarting the OnBoard

When an administrative user goes to Mgmt → Restart, the screen shown in the following figure appears.

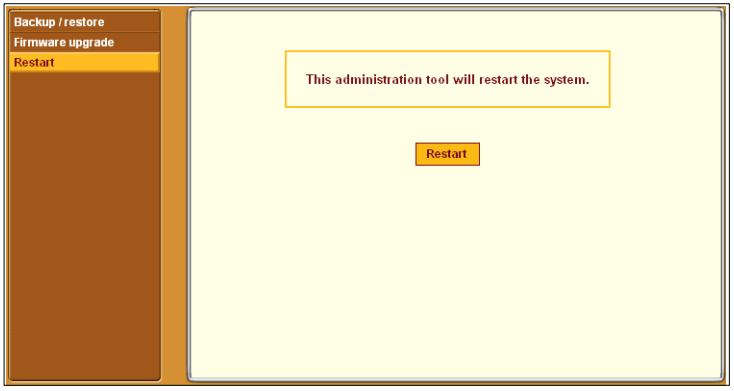


Figure 8-9: Mgmt → Restart Screen

▼ To Restart the OnBoard

1. Log into the Web Manager as an administrative user.

   See “To Log Into the Web Manager” on page 75, if needed.

2. Go to Mgmt → Restart.
3. Click the “Restart” button.

Chapter 9
Using the cycli Utility

This chapter describes the `cycli` configuration utility that is available for OnBoard administrators to use on the OnBoard's command line. This chapter covers the topics shown in the following table.

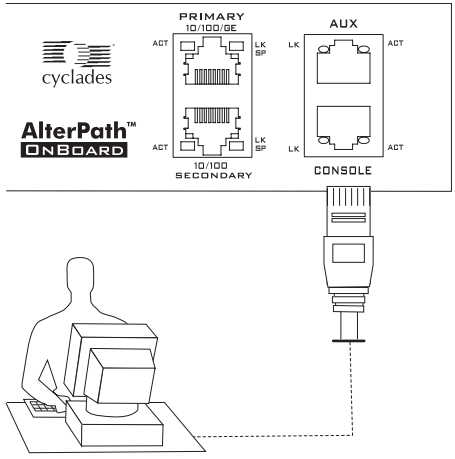
Accessing the Command Line	Page 276
`cycli` Utility Overview	Page 277
Execution Modes	Page 277
Command Line Mode	Page 278
Batch Mode	Page 278
Interactive Mode	Page 278
`cycli` Options	Page 279
`cycli` Parameters and Arguments	Page 279
Autocompletion	Page 279
Entering a Command in Interactive Mode	Page 281
Entering a Command in Command Mode	Page 282
Entering a Command in Batch Mode	Page 282
`cycli` Commands	Page 285

Accessing the Command Line

As described in the *AlterPath OnBoard User's Guide*, administrators can access the OnBoard command line in any of the following three ways.

- By local logins through the console port

  Local OnBoard root users can access the command line by logging in through the console port using a terminal or computer running a terminal emulation program, as illustrated in the following figure.



- By remote logins using SSH or PPP or a terminal emulation program

  Remote users can access the OnBoard command line through `ssh` or by using a terminal emulation program to dial into an external modem or by creating a PPP connection with external modem or with a PCMCIA modem card.

- By clicking "OnBoard" after logging into the Web Manager.

  After logging into the Web Manager, remote users can access the command line by clicking the "OnBoard" menu option.

cycli Utility Overview

An administrator (root or admin) can configure the OnBoard using the cycli utility. Only one administrator (root or admin) can run the cycli utility at a time. While in the cycli utility, the administrator can escape to the shell and when finished can return to the cycli utility.

Administrators often prefer using the cycli over the Web Manager because they can run frequently-performed cycli configuration commands from shell scripts or from text files that can be executed in batch mode. For example, on an OnBoard with forty private Ethernet ports, configuring all the service processors one by one could be tedious and prone to error, so scripting the configuration of multiple service processors is a good use of the cycli utility. Example scripts are provided in /libexec/example_scripts.

The cycli utility provides a set of commands (described under “cycli Commands” on page 285**)**. The commands act on parameters that are nested in a format called the CLI parameter tree. Some parameters require arguments when the parameters are entered with some commands. (How to find out which parameters need which arguments is shown under “cycli Parameters and Arguments” on page 279.)

Note: This section describes the cycli command and how to navigate the cycli parameter tree, but it does not describe all the parameters and values. For examples of how to use the cycli command for performing tasks such as adding users and groups, configuring devices, and authentication, see examples in /libexec/example_scripts.

Execution Modes

The cycli utility has the following three modes:

- Command line
  See “Command Line Mode” on page 278
- Batch
  See “Batch Mode” on page 278
- Interactive
  See “Interactive Mode” on page 278

Command Line Mode

Command line mode refers to when the `cycli` utility is invoked on the Linux command line with options, commands, and parameters and values.

The `cycli` utility performs the specified commands, displays any values requested by a command (such as the "`get`" command), and returns the shell prompt. To commit the changes made in command line mode, make sure to use the `-C` option as part of the command line. See "Entering a Command in Command Mode" on page 281.

When invoked without commands, `cycli` enters *interactive mode*; see Interactive Mode." When the `cycli` utility is invoked the `-f` *file* option, or it is invoked from a script, the commands are executed in *batch mode* from the specified file or script. See "Batch Mode" on page 278.

Interactive Mode

Entered by invoking `cycli` on the command line. The `cli>` prompt appears, and the administrator performs configuration by entering commands followed by parameters followed by parameter arguments at the `cli>` prompt. The `cycli` utility waits for new commands until the user enters the `exit` command. See "Entering a Command in Interactive Mode" on page 281.

Batch Mode

Refers to invoking `cycli` commands from a file as follows:

- `cycli` commands can be saved in a plain text file and executed in batch mode by invoking the `cycli` utility with the `-f` *file* option.
- `cycli` commands can be used in any kind of shell script:
  - #!`/usr/bin/cycli` can he invoked at the top of a shell script if the script contains only `cycli` commands.
  - Any type of shell can be used to run `cycli` commands along with other commands.

See "Entering a Command in Interactive Mode" on page 281.

cycli Options

Administrators can invoke the cycli command with a number of different options shown in the following table.

Table 9-1: cycli Utility Options

Option	Description
-1	When entered either in command line or in batch mode with commands that act on a single parameter, speeds up response time.
-C	Commits changes when quitting.
-f *file*	Reads commands from file. Used for running commands in batch mode.
-F	Forces login (terminate an existing configuration session, if any). Used when specifying commands to run in command line or batch mode.
-h	Help. Shows a brief summary of command line options.
-q	Quiet mode. Suppresses messages. Useful only when entering interactive mode.
-t *timeout*	Sets the idle timeout in minutes. Default is 10 minutes.
-T	Disables idle timeout (same as -t 0).
-V	Displays the cycli version and exits.
--	Signals the end of options and start of cycli commands. If any are specified, cycli goes into command line or batch mode.

cycli Parameters and Arguments

The OnBoard CLI configuration options are organized in a hierarchy called a parameter tree. You can use the get, show, and list commands to show parameters (see “get | show” on page 289 and “list” on page 291). You can also use the get command to show the values of individual parameters at the end of a branch.

No tools is provided to find out which parameters let you add parameters to them, and no way exists to find out what values are accepted when setting

parameters. Expert users can look up which branches allow parameters in the /etc/param.conf file.

The following diagram illustrates one parameter in the OnBoard cycli parameter tree. As shown in the example in Figure 9-1, each branch in the parameter tree is made up of one or more parameters, one nested below the other. In the figure, the top-level network parameter is followed by the second-level interface parameter, which is then followed by the third-level failover parameter. No parameters are nested under failover.

Figure 9-1: Example Branch in the cycli Parameter Tree

In this branch the only commands supported are "get" and set." All of the parameters in a branch are entered together on a single cycli command line. For example, to get the value set for failover, you would enter:

```
cli> get network interface failover
no
cli>
```

Entering "set" with "yes" enables Ethernet failover; "no" disables it. To set failover, you would enter the following command in interactive mode:

```
cli> set network interface failover
yes
OK
cli>
```

You can use autocompletion with the set command to find out the accepted values.

```
cli> set network interface failover <Tab><Tab>
set to yes or no. Enables or disables the interface bond0.
cli>
```

Entering Values With Parameters

Enter values that contain spaces within double quotes (“). To set a value that contains double quotes, precede the double quote within a double quote with a backslash (\), which is achieved by typing two backslashes.

To add a user called “mozart” and to set the value of the user’s GECOS to “Wolfgang Amadeus “Wolfie” Mozart, \\ “Vienna, Austria” //,” you would enter the following:

```
cli> add onboard user mozart

OK

cli> set user mozart gecos “Wolfgang Amadeus \”Wolfie\” Mozart,
\\\\\”Vienna, Austria\”\/\/\”

OK
```

Entering a Command in Interactive Mode

Based on the branch in the example in Figure 9-1, you could enter the `set` command with the following parameters in interactive mode to turn on Ethernet failover.

```
[admin@onboard /home/admin]# cycli

cli> set network interface failover yes
```

Entering a Command in Command Mode

Based on the branch in Figure 9-1, you could enter the `set` command to turn on Ethernet failover with the parameters shown in the following screen example in command mode. When the command completes, the shell prompt returns. The backslash in the example indicates that the command is too long for the page format. On the command line, you could enter all the parameters together with the value on the same command line.

```
[admin@onboard /home/admin]# cycli -CF1 set network \
interface failover yes
```

Entering a Command in Batch Mode

Based on the example in Figure 9-1, you could use batch mode to turn on Ethernet failover as shown in the following examples

You could put the command in a script that calls /usr/bin/cycli with the -CF options, as shown in the following screen example.

```
#!/usr/bin/cycli -CF
set network interface failover yes
```

You could then make the script executable and execute it on the command line, as shown in the following screen example.

```
[root@onboard root]# chmod 777 scriptname
[root@onboard root]# ./scriptname1
```

If you want to run a cycli command from the same script that is running other Linux commands, you could put the command in another type of shell script. The bash shell is shown in the following example:.

```
#!/bin/bash
...
/usr/bin/cycli -CF -- set network interface failover yes
...
```

If you want to run multiple `cycli` commands from a script that is also running other Linux commands, you could add the multiple `cycli` commands as shown in the following example:.

```
#!/bin/bash
...
/usr/bin/cycli << EOF
set network interface failover yes
set network hostname frutabaga
commit
EOF
```

You could then make the script executable and execute it on the command line, as shown in the following screen example.

```
[root@onboard root]# chmod 777 scriptname2
[root@onboard root]# ./scriptname2
```

You can put one or more commands in a plain text file without invoking any shell as shown in the following screen example.

```
set network interface failover yes
```

And then you can invoke the `cycli` command with the `-f file` option to execute the command(s) from the *`file`*, as shown in the following example.

```
[root@onboard root]# cycli -f filename
```

Autocompletion

Autocompletion can be used to find out what commands and parameters are available. Pressing the Tab key displays all the commands at the top level, as shown in the following screen example.

```
cli> <Tab>
add    commit   exit  list   rename    set   show
cd     delete   get   quit   revert    shell version
```

Typing any of the commands such as `add` or `set` then pressing Tab twice displays all the top level parameters, as shown in the following screen example.

```
cli> set <Tab><Tab>
auth           httpd          ntp            sensoralarm    user
auxport         ipdu           onboard        service         web
bootconf        ipsec           param          snmpd
cards           iptables        pptpd          sshd
```

Pressing the Tab key once after partially-typing a parameter name automatically completes the parameter name, unless there is more than one parameter name beginning with the typed characters. If more than one parameter name begins with the typed characters, then Tab Tab displays them all.

Example:

```
cli> s<Tab> <Tab>
set   shell   show
cli> se<TAB>
cli> set n<TAB><TAB>
network notifications ntp
cli> set ne<TAB>
cli> set network <TAB><TAB>
hostname hosts interface resolv smtp st_routes
cli> set network i<TAB>
cli> set network interface eth0 <TAB><TAB>
active address broadcast gateway method mtu netmask
cli> set network interface eth0 ac<TAB>
cli> set network interface eth0 active <TAB>
enable or disable eth0 with yes or no
cli> set network interface eth0 active <ESC><TAB>
cli> set network interface eth0 active yes <TAB><TAB>
active address broadcast gateway method mtu netmask
cli> set network interface eth0 active yes b<TAB>
cli> set network interface eth0 active yes broadcast
10.0.0.255<Enter>
OK
cli>
```

cycli Commands

The cycli utility supports the commands that are listed in the following screen example, which are described in the following sections with examples.

```
cli> <Tab><Tab>
add    commit  exit  list   rename    set   show
cd     delete  get   quit   revert    shell version
```

add

The add command adds the last parameter and sets it to the default value (if any). Any non-default values must be added using the set command.

add *parameter(s) value*

The add command is used instead of set when multiple parameters of the same type can exist. For example, add network hosts *IP address* makes an entry for a host with the specified IP address in the hosts list. In that case, add is used because multiple hosts can exist.

In contrast, the set command (set network interface eth0 *IP address)* is used to specify the IP address for one of the Ethernet interfaces. In that case, the set command is used because each interface has only one IP address.

Adding certain parameters causes one or more related parameters to be added. For example, in the case where an IP address is added to the hosts list, empty hostname and alias parameters are also added. Until values are set for empty parameters, the get or show commands list the parameter names without any values.

Also as shown in the screen example, you must add parameters in a prescribed order. Because the empty hostname and alias parameters are created when you add a host's IP address, you cannot add a host by name before specifying the host's IP address, and you cannot specify the host name at the same time as its IP address. To specify a name or alias for a host you need to add the host first by adding its IP address, then you need to use the set command to specify its name and alias.

Example:

```
cli > set network hosts 192.168.160.11 name fruitbat
ERR result=5 No such file or directory
cli > get network hosts 192.168.160.11 name fruitbat
ERR result=5 No such file or directory
cli > add network hosts 192.168.160.11
OK
cli > get network hosts 192.168.160.11
name
alias
cli > set network hosts 192.168.160.11 name fruitbat alias
fbat
OK
cli > get network hosts 192.168.160.11
network hosts 192.168.160.11 name: fruitbat
network hosts 192.168.160.11 alias: fbat
```

cd

Set a parameter prefix for subsequent commands. The prompt then changes to indicate the prefix. Entered by itself, `cd` returns to the top level.

Example:

```
cli> cd network
network> get hostname
dingo
network> set hostname kookaburra
OK
network> cd interface eth0
network interface eth0> set
active    address   alias     broadcast  gateway   method
mtu        netmask
ip address for interface eth0
netmask for interface eth0
network interface eth0> set address 192.168.160.10 netmask
255.255.255.0
OK
network interface eth0> cd ..
network interface> cd eth1
network interface eth1> set address 192.168.50.10
OK
network interface eth1> cd
cli>
```

commit

Saves changes in configuration files and creates a compressed copy of the configuration files in a backup directory.

Note: If you make a change but do not commit it, the configuration files will not be updated, and your changes will be lost after the next reboot.

delete

Deletes the last parameter in the command line. Deleting certain parameters deletes associated parameters. For instance, if an IP address is deleted from the host list, other parameters associated with a host (name, alias) are also deleted.

`delete` *`parameter(s)`*

Some parameters cannot be deleted. Parameters that can be added can be deleted.

Example:

```
cli> get network hosts 192.168.160.11
network hosts 192.168.160.11 name fruitbat alias fbat
cli> delete network hosts 192.168.160.11
OK
cli> set network hosts 192.168.160.11 name: fruitbat
ERR result=5 No such file or directory
cli> get network hosts 192.168.160.11 alias: fbat
ERR result=5 No such file or directory
```

exit

See “quit | exit” on page 292.

get | show

Get the value assigned to a parameter. When no parameters are listed, the whole parameter tree is displayed. If full parameters are specified, the assigned value is displayed.

```
get | show parameter(s)
```

Example:

```
cli > get network hostname
anchovy
cli> show network resolv domain
cyclades.com
```

When get is entered with a partial parameter, all the subtrees display. In the output, if a value is assigned, the parameter preceding the value ends with a semicolon.

Example:

```
cli > get network
network interface failover: no
network interface eth0 active: yes
network interface eth0 method: dhcp
network interface eth0 address: 192.168.160.10
network interface eth0 netmask: 255.255.255.0
network interface eth0 broadcast: 192.168.160.255
network interface eth0 gateway: none
network interface eth0 mtu: 1500
network interface eth1 active: no
network interface eth1 method: dhcp
network interface eth1 address
network interface eth1 netmask
network interface eth1 broadcast
network interface eth1 gateway: none
network interface eth1 mtu: 1500
network interface bond0 active: no
network interface bond0 method: static
network interface bond0 address: 192.168.160.10
network interface bond0 netmask: 255.255.255.0
network interface bond0 broadcast: 192.168.160.255
network interface bond0 gateway: none
network interface bond0 mtu: 1500
network interface priv0 active: yes
network interface priv0 method: manual
network interface priv0 address
network interface priv0 netmask
network interface priv0 broadcast
network interface priv0 gateway: none
network interface priv0 mtu: 1500
network interface eth2 active: no
...
network smtp auth method
network ipv4 icmp echo_ignore_all: 0
network ipv4 ip forward
cli>
```

If the system assigns default values, default values are shown next to the automatically added parameter name, as in the following example, which was entered on the OnBoard before any configuration has been done.

Example:

```
cli> get network interface eth0
network interface eth0 active: yes
network interface eth0 method: dhcp
network interface eth0 address: 192.168.160.10
network interface eth0 netmask: 255.255.255.0
network interface eth0 broadcast: 192.168.160.255
network interface eth0 gateway: none
network interface eth0 mtu: 1500
cli>
```

Note: If you make a change but do not commit it (see “commit” on page 288), the configuration files are not updated. The get command shows the changes that are currently stored in the RAM memory, not the actual value stored in the affected configuration file.

list

List available parameters. With no parameters listed, the whole parameter tree is displayed. If parameters are specified, the corresponding subtree is displayed.

```
list [parameter(s)]
```

Example:

```
cli> list network hosts
network hosts 127.0.0.1 name
network hosts 127.0.0.1 alias
network hosts 192.168.160.10 name
network hosts 192.168.160.10 alias
```

quit | exit

Quit cycli. (Ctrl+d also quits the cycli utility.) If changes have not been committed, the user is prompted to commit the changes or quit without committing.

Example:

```
cli> set network hostname frutabaga
OK
cli> quit
You have made changes but haven't committed them yet.
To commit the changes, use the "commit" command.
To revert all changes and quit without committing, use
"quit!".
cli> commit
cli> quit
```

quit!

Quit the cycli utility, discarding any uncommitted changes.

rename

Rename a parameter. Depending on the parameter, this may result in a whole subtree of parameters being moved. For instance, if an IP address in the host list is changed, all parameters associated with that host (name, alias) are moved under the new name.

Example:

```
cli> get network hosts 192.168.160.11
network hosts name: fruitbat
alias
cli> rename network hosts 192.168.160.11
192.168.160.222
OK
cli> get network hosts 192.168.160.11
ERR No such file or directory
cli> get network hosts 192.168.160.222
name fruitbat
alias
```

revert

Discard changes and revert to previously committed state.

Example:

```
cli> get network hostname
dingo
cli> set network hostname kookaburra
OK
cli> get network hostname
kookaburra
cli> revert
OK
cli> get network hostname
dingo
```

set

Set the value(s) of the last parameter. When multiple parameters are specified in one command, either all are set successfully or none of the values are changed.

```
set parameter(s) value(s)
```

Example:

```
cli> set network resolv dns0 10.0.0.1
OK
cli> set network interface eth1 active yes address 10.0.0.3
netmask \  255.255.255.0 broadcast 10.0.0.255
OK
cli> set network interface eth0 active yes eth1 active yes
ERR sanity check failed
```

The `set` command is used to set an existing value, in contrast to `add` which is used to add something to the parameter tree. For example, the `set` command is used to specify the IP address for an Ethernet interface: `set network interface eth0` *IP address*. In contrast, new hosts need to be added with the add command before their parameters can be specified; `add network hosts` *IP address* makes an entry for a host with the specified IP address in the `hosts` list. Parameters for this new host can be changed with the set command: `set network hosts` *IP address* name *hostname*.

shell

Escape to shell. This command is only available to root.

Example:

```
cli> shell
[root@onboard root]# whoami
root
[root@onboard root]# logout
cli>
```

version

Displays the current `cycli` version.

Example:

```
cli> version
OnBoard CLI 2.0 (2005-06-16T13:47+1000)
```

Summary of How to Configure the Top Level Parameters

The following table is a brief overview of how to configure the top level parameters.

Typing any of the commands such as `add` or `set` then pressing Tab twice displays all the top level parameters, as shown in the following screen example.

```
cli> set <Tab><Tab>
auth        httpd      notifications  profile       syslog
auxport     ipdu        ntp             sensoralarm  timezone
bootconf    ipsec      onboard        service       user
cards       iptables   param          snmpd         web
group       network    pptpd          sshd
```

The following table shows which of the top-level parameters that you can set without using the `add` command first, and the parameters that need to be added using the `add` command first before using the `set` command to set additional parameters and values.

Table 9-2: Top Level `cycli` Parameters With Set or Add Commands (Sheet 1 of 8)

Parameter	Command
auth	• Use the `set` command to set an authentication type for logins to the OnBoard (`set auth type` *authtype*). • Use the `set` command to configure authentication server parameters (`set auth authtype` *type* <Tab><Tab> shows you what you need to set for the server's specified authtype).

Table 9-2: Top Level `cycli` Parameters With Set or Add Commands (Sheet 2 of 8)

Parameter	Command
auxport	• Use the `set` command to configure the AUX port for a connected modem or ipdu (`set auxport profile modem | ipdu`). If the `modem` profile is set, use the set command to configure the modem (`set auxport modem` <Tab><Tab> shows the modem configuration parameters to set)
bootconf	Use the `set` command to configure boot configuration (`set bootconf` <Tab><Tab> shows the boot configuration parameters to set).
cards	Use the `set` command to configure PCMCIA cards (`set cards` <Tab><Tab> shows the *cardtypes*, and `set cards` *cardtype* <Tab><Tab> shows the configuration parameters to set).[1]
group	Use the `add` command to add a group (`add group` *groupname*). A GID is automatically set. Use the `set` command to configure the group members (`set group` *groupname* `users` *username[,username2,...,usernameN*)
httpd	Use the `set` command to configure HTTP/ HTTPS services (`set httpd http Tab Tab` shows the configuration parameters to set)

Table 9-2: Top Level `cycli` Parameters With Set or Add Commands (Sheet 3 of 8)

Parameter	Command
ipdu	• Use the `set` command to configure an IPDU (`set ipdu s1 <Tab><Tab>` shows the configuration parameters to set) • Use the `set` command to configure the outlets (`set ipdu s1 <Tab><Tab>` shows the configuration parameters to set) • Use the `add` command to add users who can configure outlets (`add ipdu s1 users` *`username`*) • Use the `set` command to configure which outlets each user can manage (`set ipdu s1 users` *`username`* `<Tab><Tab>` shows the configuration parameters to set)
ipsec conn	• Use the `add` command to add a VPN IPSec connection name (`add ipsec conn` *connectionname*). • Use the `set` command to configure the connection parameters (`set ipsec conn` *`connection_name`* <Tab><Tab> shows the configuration parameters to set)
iptables [filter | nat]	By default, a set of chains is defined but no rules are configured: For NAT, the predefined chains are: PREROUTING, POSTROUTING, OUTPUT. For filter, the predefined chains are: INPUT, OUTPUT, FORWARD. • Use the `add` command to add a chain of type filter or nat (`add iptables [filter | nat]` *connectionname*). • Use the `set` command to configure the parameters (`set iptables [filter | nat]` <Tab><Tab> shows the configuration parameters to set).

Table 9-2: Top Level `cycli` Parameters With Set or Add Commands (Sheet 4 of 8)

Parameter	Command
network hostname	• Use the `set` command to configure the OnBoard hostname (`set network hostname` *`OnBoard_hostname`*)
network hosts	• Use the `add` command to add a host to the hosts table (`add network hosts` *IP_address*). • Use the `set` command to configure the host (`set network hosts` *IP_address* <Tab><Tab> shows the parameters to set)
network interface	Use the `set` command to configure one of the network interfaces (`set network interface` <Tab><Tab> lists the interfaces to configure; `set network interface` *interface_name* <Tab><Tab> lists the parameters to configure)
network ipv4	Use the `set` command to configure ipv4 (`set network ipv4` <Tab><Tab> lists the parameters to configure)
network resolv	Use the `set` command to configure DNS (`set network resolv` <Tab><Tab> lists the parameters to configure)
network smtp	Use the `set` command to configure email notifications to be sent to root (`set network smtp` <Tab><Tab> lists the parameters to configure)
network st_routes	• Use the `add` command to add a static route to the routing table (`add network st_routes` *IP_address*). • Use the `set` command to configure the static route (`set network st_routes` *IP_address* <Tab><Tab> shows the parameters to set)

Table 9-2: Top Level `cycli` Parameters With Set or Add Commands (Sheet 5 of 8)

Parameter	Command
notifications	• Use the `add` command to add a notification (`add notifications` *name*). • Use the `set` command to configure the parameters (`set notifications` *name* <Tab><Tab> shows the parameters to set)
ntp	Use the `set` command to specify the IP address of an NTP server (`set ntp` *IP_address*)
onboard global default authtype	Use the `set` command to configure the authentication method for OnBoard logins (`set onboard global default authtype` *authentication_method)*
onboard global security encrypt-passwords	Use the `set` command to configure whether passwords are encrypted; the default is “no” (`set onboard global security encrypt_passwords [yes | no])`
onboard global security override_authorization	Use the `set` command to configure whether authorizations are ignored when users attempt to access devices; the default is “no” (`set onboard global security override_authorizations [yes | no])`
onboard group	• Use the `add` command to configure an onboard group (`add onboard group` *groupname)* • Use the `set` command to configure the parameters (`set onboard group` *servername* <Tab><Tab> shows the parameters to set)

Table 9-2: Top Level `cycli` Parameters With Set or Add Commands (Sheet 6 of 8)

Parameter	Command
onboard server	• Use the `add` command to configure a device (`add onboard server` *servername)* • Use the `set` command to configure the parameters (`set onboard server` *servername* <Tab><Tab> shows the parameters to set)
onboard user	• Use the `add onboard user` command to configure a user (`add onboard user` *username)* • Use the `set user` command to configure the normal Linux user's parameters such as passwd (`set user` *username* <Tab><Tab> shows the parameters to set). • Use the `add onboard user` command to authorize a user to use a device that has been previously configured—possibly with `set onboard server` *devicename* (`add onboard user` *username devicename)* • Use the `set onboard user` *username devicename* command to specify which device management actions the user can perform on the device (`set onboard user` *username devicename* <Tab><Tab> shows the device management actions to set by specifying `yes` or `no` for each).
pptpd	Use the `set pptpd` command to configure PPTP (`set pptpd` <Tab><Tab> shows the parameters to set).
profile	Use the `set profile` command to select the security profile (`set profile` Tab Tab shows the parameters to set).

Table 9-2: Top Level `cycli` Parameters With Set or Add Commands (Sheet 7 of 8)

Parameter	Command
sensoralarm	• Use the `add sensoralarm` command to configure a sensor alarm (`add sensoralarm` *alarm_ID)* • Use the `set sensoralarm` command to configure the parameters (`set sensoralarm` *alarm_ID* <Tab><Tab> shows the parameters to set).
service	Use the `set service` command to enable or disable any service (`set service` <Tab><Tab> shows the services to enable or disable by specifying `enable yes` or `enable no` for each).
snmpd [access | com2sec | group | user | view]	• Use the `add snmpd` command to add access, com2sec, group, user, and view (`add snmpd [access | com2sec | group | user | view]` • Use the `set snmpd` command to configure the parameters (`set snmpd` *parameter* Tab Tab shows the parameters to set).
sshd	Use the `set sshd` command to enable or disable SSHD (`set sshd` <Tab><Tab> shows the parameters to set).
syslog	Use the `set syslog` command to specify a syslog server (`set syslog` <Tab><Tab> shows the parameters to set).
timezone	Use the `set timezone` command to specify the timezone (`set timezone` <Tab><Tab> shows the parameters to set)

Table 9-2: Top Level `cycli` Parameters With Set or Add Commands (Sheet 8 of 8)

Parameter	Command
user	• Do not use this command to add a user. Use `add onboard user` *username* first. • Use the `set user` command to configure the normal Linux user's parameters such as the passwd (`set user` *username* <Tab><Tab> shows the parameters to set).
web	Use the `set web` command to specify a user-accessible server where the help files have been downloaded (`set web` <Tab><Tab> shows the parameter to set). The default is http://www.cyclades.com/online-help/onb/v_1.0.0/.

1. For this release, `ethernet`*N* and `modem`*N* are the only card types that are supported.

Chapter 10
Troubleshooting

This chapter provides information related to troubleshooting the OnBoard.

See the sections shown in the following table.

Connection Methods for Troubleshooting	Page 304
Recovering from root Authentication Failure	Page 304
Restarting the Web Manager	Page 306
Replacing a Boot Image for Troubleshooting	Page 307
Using the create_cf Command When Troubleshooting	Page 307

This chapter also provides the troubleshooting procedures shown in the following sections.

To Recover from root Authentication Failure	Page 305
To Restart the Web Manager	Page 306

See also Appendix A, “Advanced Device Configuration,” for procedures to use if you have trouble getting connected devices to communicate with the OnBoard.

Connection Methods for Troubleshooting

This section summarizes how to connect to the OnBoard for troubleshooting in the event of an IP network failure.

Remote OnBoard administrators can connect to the OnBoard in case of network failure in any of the following ways:

- By bringing up the Web Manager or logging into the OnBoard's console over PPP after establishing a dial-in or callback connection to either of the following modem types:
  - An external modem optionally connected to the OnBoard
  - A modem on a PCMCIA modem card optionally installed in the OnBoard
- By logging into the OnBoard's console after establishing a dial-in connection from a terminal emulation program to an external modem optionally connected to the OnBoard

Local OnBoard administrators can connect to the OnBoard by logging into the Linux command line through a terminal or computer that is connected to the OnBoard's console port.

All of these connection methods must be previously configured as described elsewhere in this manual. For example, to enable use of a PCMCIA modem card, the PCMCIA modem card must be installed as described in the *AlterPath OnBoard Installation Guide* and configured as described in c.

Recovering from root Authentication Failure

Use the following procedure if an attempt to login to the console as root brings up the following message.

```
login[212]: FAILED LOGIN
1 FROM  FOR root, User not known to the underlying
authentication module
Login incorrect
```

▼ *To Recover from root Authentication Failure*

1. Boot the OnBoard in the u-boot monitor mode.

   See "To Boot in U-Boot Monitor Mode" on page 377. The U-Boot monitor prompt appears as shown in the following screen example:

```
=>
```

2. After you log in, open the `/etc/nsswitch.conf` file for editing.

```
[root@ONS root]# vi /etc/nsswitch.conf
```

3. Search for the uncommented entries for the `passwd`, `shadow` and `group` databases [whose lines do not start with the pound (#) sign].

   For example, in the portion of the `nsswitch.conf` file in the following screen example, no pound (#) signs appear before the entries for the `passwd`, `shadow`, and `group` databases under `NISLocal`.

```
# NISLocal
passwd:     nis files
shadow:     nis files
group:      nis files
```

4. Change the search order to `files` only for the uncommented `passwd`, `shadow`, and `group` databases.

```
# NISLocal
passwd:     files
shadow:     files
group:      files
```

5. Save and quit the file.

6. Open the `/etc/portslave/pslave.conf` file for editing.

```
[root@ONS root]# vi /etc/portslave/pslave.conf
```

7. Change the `conf.authtype` parameter back to `local`.

```
# by default, authentication to the box is local
conf.authtype   local
```

8. Save and quit the file.
9. Restart the OnBoard to return to multiuser mode.

```
[root@ONS root]# reboot
```

   You should be able to log in as root.

10. Reconfigure authentication as desired.

Restarting the Web Manager

If the Web Manager stops responding you can perform the following procedure to restart the Apache web server.

▼ *To Restart the Web Manager*

1. Enter the `http -k start` command as shown in the following screen example.

```
[root@OnBoard root]# /usr/local/apache2/bin/httpd -k start
```

2. Enter the `ps` command with the `-ef` option and look for a line with `apache`, as shown in the following screen example.

```
[root@OnBoard root]# ps -fe | grep apache
10131 nobody   3864 S  /usr/local/apache2/bin/httpd -k start
```

   If a line like the one shown in the previous screen example appears, the web application successfully restarted.

Replacing a Boot Image for Troubleshooting

Information in “Boot File Location Information” on page 372 in Appendix B, “Advanced Boot and Backup Configuration Information” gives an OnBoard administrator who has the root password enough background to be able to boot from an alternate image if the need arises and if the Web Manager is not available.

Network boots are recommended for troubleshooting. For example, if you want to test a new release of the software to make sure a problem is fixed, or if the removable flash memory becomes corrupted, you could download the software to a tftpboot server, and then save it to the removable flash after testing, using the `create_cf` command.

Using the create_cf Command When Troubleshooting

You can use the `create_cf` command when troubleshooting problems with the boot image, as described under “To Replace a Boot Image From a Network Boot in U-Boot Monitor Mode” on page 379. Use it carefully as described in the referenced section.

Appendix A
Advanced Device Configuration

This appendix provides detailed information needed to understand how to configure a new device.

See the sections listed in the following table.

OnBoard-specific Tasks for Configuring New Devices	Page 310
Understanding How the OnBoard Manages Communications With Devices	Page 311
Understanding Address Configuration for Connected Devices	Page 336

This chapter also provides the procedures listed in the following table.

To Find Out if An Existing Command Template Works With a New Device	Page 317
To Use the onbdtemplate Utility to Create a New Template	Page 318
To Use the onbdtemplate Utility to Test a Template	Page 320
To Create a Custom Expect Script	Page 336
To Create a Custom IPMI Expect Script	Page 333

OnBoard-specific Tasks for Configuring New Devices

The following device configuration requirements are unique to the OnBoard:

- During device configuration, the OnBoard administrator must assign a *command template* to each device.
- The OnBoard administrator must also assign each device a *private subnet*, except in exceptional cases.
- The OnBoard administrator may need to assign to each device a *virtual IP address*, which hides the real IP address of the device from users, and which requires the configuration of a virtual network (DNAT)

The following table lists the sections that apply to each requirement.

Table A-1: OnBoard-specific Tasks for Configuring New Devices

Configuration Parameter	Where Documented
Assigning command templates and device types	• "Understanding How the OnBoard Manages Communications With Devices" on page 311 • "Device Type Differences" on page 312 • "Assigning a Command Template to a New Device" on page 316 • "Command Templates" on page 321 • "Issues Affecting the Configuration of RSA-Type Service Processors" on page 325 • "The onbdtemplate Utility" on page 325 • "OnBoard Expect Scripts" on page 329

Table A-1: OnBoard-specific Tasks for Configuring New Devices (Continued)

Configuration Parameter	Where Documented
Creating and assigning IP addresses of the following types: • A device IP address • A virtual IP address • A private subnet • A optional virtual network (DNAT) address	• "Understanding Address Configuration for Connected Devices" on page 336 • "Using Reserved IP Addresses for Private IP Addressing" on page 338 • "Why Define Private Subnets?" on page 339 • "Configuring a Private Subnet" on page 340 • "Routing Requirements for Native IP Access" on page 341 • "Example 1: Private Subnet Configuration" on page 342 • "Example 2: Two Private Subnets and VPN Configuration" on page 345 • "Why Define Virtual (DNAT) Addresses?" on page 357 • "Example 3: Virtual Network With Two Private Subnets and VPN Configuration" on page 358 • "Additional Network Address Configuration Examples" on page 368

Understanding How the OnBoard Manages Communications With Devices

The OnBoard uses *Expect scripts* to handle communications with connected devices. One Expect script is provided to interact with each supported device type using text-based interfaces. The text-based interfaces are defined in a separate *command template* for each device type. The Expect scripts use the command templates to log into the devices and perform device management actions on behalf of authorized users.

The OnBoard has been tested with specific models of devices and firmware levels that are listed in the release notes (at `http://www.cyclades.com/support/downloads` under the product name "AlterPath OnBoard").

The device models and firmware in the release notes have been proven to work with the default set of command templates and Expect scripts.

The default command templates do not always work for all devices of the same type because service processors of the same type often do not use the same syntax for their commands. For example, while `power on` is the command string that works to power on a server with some RSA II type service processors, `power -on` is the command string that works with some other RSA II type service processors.

Because the default templates and scripts cannot be guaranteed to apply to all service processors of the same type, this appendix provides information about how OnBoard administrators can test command templates and create new command templates if needed to deal with command differences.

An OnBoard administrator (`root` or an administrative user) can use the `onbdtemplate` utility on the command line to test the default command templates when configuring a device and to create a customized command template if needed. Because changes to the commands that are sent to devices can be made and stored in new command templates, OnBoard administrators can accommodate devices that do not work with the default Expect scripts and templates, without having to write custom Expect scripts in most cases.

Application notes in the `/usr/share/docs/OnBoard/Application_Notes/Service_Processor_Related` directory provide additional information not provided here. Check for updated application notes at `http://www.cyclades.com/support/downloads.php` under the product name “AlterPath OnBoard.”

Device Type Differences

The device type differences are summarized in the following table. Some of the device type differences that may need to be addressed by creating new templates or Expect scripts are described in the table. See also the additional information in the `Troubleshooting.txt` file under: `/usr/share/`

`docs/OnBoard/Application_Notes/Service_Processor_Related`. Also see the `Readme.txt` file.

Table A-2: Device Type Differences

Protocol	Device Type Differences
DRAC	DRAC III/XT is the only version tested and proven to work with the default DRAC Expect script and command template. Compatibility with DRAC II or IV service processors is not guaranteed. Some DRAC service processors support sensors; modifications to the default DRAC template would be needed to support sensors; modifications to the default DRAC Expect script would be needed to take advantage of sensor alarms.
IPMI 1.5	Works without a command template and with the default scripts.
IPMI 2.0	The OnBoard administrator can support IPMI 2.0 type service processors with the IPMI 2.0 RCMP+ encrypted protocol in either of the two following ways: • Identify the service processor as a IPMI 1.5 type which enables the OnBoard to communicate with the 2.0-type service processor in "v1.5 compatibility mode." • Copy the `talk_generic_ipmi.exp` onto `talk_custom`*N*`.exp` and follow the directions within the file to modify the script for IPMI 2.0 support. • Modify the default `ipmi` script to support OEM extensions See the following application note • `IPMI_2.0.txt`
RSA I	The RSA I card uses a curses-based interface. The OnBoard administrator can try to enable authorized users to perform IBM service processor console, power, and event log device management actions through a RSA I type service processor by copying the `talk_rsa_I.exp` Expect script to `talk_custom`*N*`.exp` and following the directions within the script to modify the script for RSA I support. As stated in the `RSA_I.txt` application note, this script may not be compatible with all RSA I firmware versions, so it cannot be guaranteed to work.

Table A-2: Device Type Differences (Continued)

Protocol	Device Type Differences
RSA II	The RSA II card uses a text-based interface. The card can be used in multiple IBM server platforms, and it requires a different firmware version or each platform. Simple features, such as switching power on and off, may not function if a card does not have the correct firmware version for the server in which it resides. In the discussion below, firmware for RSA II type service processors is referred to using the convention: *version/platform*. For example, firmware `version1.03/x205`, for example, is version 1.03 for the x205 platform. The versions differ between platforms, so that a later version of firmware for one platform may not have as many RSA II features as an earlier version for another platform. A comparison of some firmware versions for various platforms follows, for example: • `1.07/x235` was released before `1.03/x306`. • `1.03/x360` is very different from `1.03/x205`. • `1.03/x205` supports neither event log nor sensors from the command line, whereas `1.03/x306` and `1.07/x235` both support event logs and sensors from the command line. • "power on" switches on the power for `1.03/x306` and `1.07/x235`, but `1.03/x205` uses "power -on". • Unknown sensor data on the `1.07/x235` is shown by using asterixes, while on the `1.03/x306` unknown sensor data is indicated by blank spaces. Two RSA templates are available: `rsa.default` and `rsa.limited.default`. The `rsa.limited.default` template is for RSA II type devices that support only power commands through the device's command line interface. A custom Expect script can be created to provide support for RSA II service processors that do not work with the default rsa command templates.See the `RSA_II.txt` file in the application notes `IBM` subdirectory.

Additional Reasons for Creating Custom Expect Scripts

The following table lists some of the reasons an administrator might want to create a custom `Expect` script.

Table A-3: Reasons for Customizing Expect Scripts

Purpose	Notes
Change the device access method from `telnet` to `ssh`, or to some other program.	Administrators would probably want to change the device access method if devices must be connected to the public ports on the OnBoard, because `telnet` is not encrypted. See "Configuring SSH or Bidilink Instead of Telnet for OnBoard to Device Connections" on page 20. Also see the following files in the `Alternate_Access` directory: • `SSH_Access.txt` • `bidilink_Access.txt` In addition, see the notes in the following files in the `/libexec/onboard` directory: • `bidi_login.exp` • `ssh_login.exp`
Interact with the web interface of a service processor	The `RSA_I.txt` file in the application notes `IBM` subdirectory and the `talk_rsa_I.exp` script address accessing the RSA I web interface, and the instructions in this file can be followed for accessing other device types' web interfaces.
Add functionality to a `devconsole`-type script to access additional features available through a device's console, such as logging in and reporting on the event log, sensors, or performing power functions.	See the `Devconsoles.txt` file in the application notes `Devconsoles` directory: If the device console supports additional management features, commands for the supported commands can be added and the default devconsole script can be updated with commands that use the supported command interfaces.

Custom scripts can also be deployed for the following purposes:

- To handle changes in service processor firmware on a supported service processor type
- To provide some limited functionality with other types of devices, including Sun ALOM, ILOM, and RSC, and IBM BladeCenter and RILOe
- To provide access to new service processor types

Assigning a Command Template to a New Device

When configuring a new device, the OnBoard administrator should not assign a command template when the device is either of the following two types of devices:

- Any IPMI-type device (IPMI devices are managed using `ipmitool` commands)
- Any device being configured only for Native IP access

When adding any other kind of new device, the OnBoard administrator needs to do the following:

- Find out if the new device and its firmware have been tested and proven to work with the applicable default command template.
- Read any application notes that relate to that type of device.
- If the new device is running untested firmware, test whether the firmware is compatible with the applicable default command template.
- If communications cannot be established with the new device using the default command template, use the `onbdtemplate` utility to create and test a new command template, after making any needed changes to the commands that manage communications between the device and the OnBoard.
- If a new template cannot be made to work, create a custom Expect script to handle the device's requirements.

See "To Find Out if An Existing Command Template Works With a New Device" for how to perform the above-listed steps.

▼ *To Find Out if An Existing Command Template Works With a New Device*

1. Check the release notes to see if the device is in the list of tested devices, and if the device is listed, to see if the device's firmware level is also listed.
   a. Navigate to `http://www.cyclades.com/support/downloads` and click on the product name "AlterPath OnBoard."
   b. Scroll down to the section heading "Firmware," then find and click the "Release Notes" link.
   c. Locate the table of tested devices and firmware levels and check the new device's model and firmware level against the list.
2. Review any application notes that relate to the type of device under `/usr/share/docs/OnBoard/Application_Notes/Service_Processor_Related`.
3. Check for updated application notes at `http://www.cyclades.com/support/downloads.php` under the product name "AlterPath OnBoard," and if any are found, review those notes for additional tips about the type of device being configured.
4. If the device and its firmware level are listed in the release notes as having been tested, assign the device the appropriate device type and the associated default command template for the device type and you are done.

   See "Default Command Templates" on page 166 for the list of command templates that apply to each type of device. See "To Add a Device" on page 166 for how to add a device using the Web Manager.
5. If the device is listed in the release notes as a tested device, but the firmware version is not the same as the one tested or if the device is not listed at all, do the following steps:
   a. Assign the device the appropriate device type and the associated default command template for the device type.
   b. Try to run power management commands on the device.

6. If the device is an RSA II type device, if you cannot run power commands on the device using the `rsa.default` template, assign the device the `rsa.limited.default` template.
7. If you can run power commands on the device, test the rest of the device management commands that are supported on the device. If they work, you are done.
8. If you cannot run one or more of the supported commands on the device, attempt to connect to the service processor console.

Note: Even if the power management commands do not work on a new device, you can usually establish a connection to the service processor's console.

---

9. If you cannot access the service processor console, do the following steps.
   a. Use `ping`, `telnet`, or `ssh` to verify that you can get to the server.
   b. If you cannot access the server, check the network configuration and fix the problem that is preventing access.
10. If you can access the server but still cannot access the service processor's console, double-check the user name and password you are using against the user name and password that are configured for the device.
11. Once you have established the connection to the service processor's console, type the `help` command, which gives you the syntax you need to use for the commands supported by the service processor.
12. Note the syntax of the commands supported by the service processor's console, and go to "To Use the onbdtemplate Utility to Create a New Template" on page 318.

▼ *To Use the onbdtemplate Utility to Create a New Template*

Perform this procedure after "To Find Out if An Existing Command Template Works With a New Device" on page 317, if the default templates do not work for a new device. See "The onbdtemplate Utility" on page 325 for details about using the `onbdtemplate` utility, if needed.

1. Log into the OnBoard's console as an administrator and run the `onbdtemplate` utility.
2. Select `New` from the menu.
3. Enter a template name, such as `rsa.new`.

   The editor brings up a template for a new command template assigning it the name you specified.
4. Enter the device type in the form "`type =` *device_type*."

   Using the syntax supported on the device, perform the following steps to fill in the commands supported by the service processor. Follow the instructions in the template you are editing.

Note: Sensors may not be supported. If any command is not supported, leave it commented out in the template.

---

5. Enter the login prompt in the form "`login_prompt =` *login_prompt*."
6. Enter the password prompt in the form "`pass_prompt =` *pass_prompt*."
7. Enter the command prompt in the form "`cmd_prompt =` *cmd_prompt*."
8. Enter the logout command in the form "`logout_cmd =` *logout_cmd*."
9. Enter the power on command in the form "`poweron_cmd =` *poweron_cmd*."
10. Enter the power off command in the form "`poweroff_cmd =` *poweroff_cmd*."
11. Enter the power cycle command in the form "`powercycle_cmd =` *powercycle_cmd*."
12. Enter the power status command in the form "`powerstatus_cmd =` *powerstatus_cmd*."
13. Enter the reset command in the form "`reset_cmd =` *reset_cmd*."
14. Enter the sensors command in the form "`sensors_cmd =` *sensors_cmd*."

15. Enter the command to read the system event log (SEL) in the form "`sel_cmd = sel_cmd`."
16. Enter the command to clear the SEL in the form "`clearsel_cmd = clearsel_cmd`."
17. Enter the command to access the device console in the form "`devconsole_cmd = devconsole_cmd`."
18. Enter the escape sequence used to escape from the console in the form "`devconsole_esc = devconsole_esc_sequence`."

Caution! You must specify the device console escape sequence to block users who are authorized for device console access from being able to escape to the service processor console whether or not they are authorized.

---

19. Save and quit the file.
20. Enter the `saveconf` command.
21. Logout from the console.
22. Log into the Web Manager as an administrative user and go to Config → Devices.

    When an administrative user logs in, the new template is automatically added to the `/etc/onboard_templates.ini` file and is included in the list of command templates that you can assign to a device.
23. Assign the new template to the device.

▼ *To Use the onbdtemplate Utility to Test a Template*

When `onbdtemplate` is used to test a template, extra debugging information is provided to report on commands sent to and received from the device. See "The onbdtemplate Utility" on page 325 for details about using the `onbdtemplate` utility, if needed.

1. Log into the OnBoard's console as an administrator and invoke the `onbdtemplate` utility.
2. Select `Test` from the menu.

3. At the prompt, confirm that you want to continue by entering "y."

   A list of templates appears.

4. Select a template to test.

   A list of configured devices appears.

5. Select a device to test the template against.

   The editor runs the commands in the specified template and returns debugging information that you can record for making command changes in a new template.

6. Choose a command to test.

7. At the prompt, enter the username and password you used when logging into the OnBoard.

8. Go to "To Use the onbdtemplate Utility to Create a New Template" on page 268.

Command Templates

Command templates are stored in the `/etc/onboard_templates.ini` file. The command templates contain text commands that are used to interact with the service processors and devices.

The following table lists the default command templates and describes type types of devices to which they apply.

Table A-4: Default Command Templates

Template	Type of Device
`devconsole.default`	Devices that support access to their consoles.
`drac.default`	DRAC type devices.
`ilo.default`	iLO type devices.
`rsa.default`	Some RSA II type devices.
`rsa.limited.default`	RSA II type devices that support only power commands through their command line interface.

Table A-4: Default Command Templates

Template	Type of Device
`no template`	• IPMI type devices • Any type device when only Native IP access is being configured

All templates in the `onboard_template.ini` file are listed in the Web Manager in the Config → Devices "Command template" pull-down menu.

If an administrator creates a new template, the new template automatically is added to the list the next time an administrative user logs into the Web Manager. An already-logged in administrative user can click the "Cancel changes" button to update the list.

The `/etc/onboard_server.ini` file stores the configuration parameters for each configured device, except for the username and password information for each device, which are stored in the `/etc/onboard_server_auth.ini` file. By default, neither file has any entries until devices are configured. The following screen example shows an example `onboard_server.ini` file that defines one device for each of the default template types.

```
[rack1_dev1_ibm_rsa]
        type = rsa_II
        ip = 10.0.0.1
        real_ip = 192.168.0.1
        local_ip = 192.168.0.254
        virtual_ip = 10.0.0.1
        netmask = 255.255.255.0
        authtype = local
        template = rsa.default
        description = IBM xSeries E306 in Fremont
```

```
[rack1_dev2_compaq_ilo]
        type = ilo
        ip = 10.0.0.2
        real_ip = 192.168.0.2
        local_ip = 192.168.0.254
        virtual_ip = 10.0.0.2
        netmask = 255.255.255.0
        authtype = local
        template = ilo.default
        description = Compaq Proliant iLO 1.82 server
[rack1_dev3_dell_drac]
        type = drac
        ip = 10.0.0.3
        real_ip = 172.10.0.1
        local_ip = 172.10.0.254
        virtual_ip = 10.0.0.3
        netmask = 255.255.255.0
        authtype = local
        template = drac.default
        description = Dell DRAC III/XT server
```

```
[rack1_dev4_newisys_ipmi]
        type = ipmi_1.5
        ip = 10.0.0.4
        real_ip = 172.10.0.2
        local_ip = 172.10.0.254
        virtual_ip = 10.0.0.4
        netmask = 255.255.255.0
        authtype = local
        description = Newisys IPMI 1.5 server
        template =
[rack1_dev5_cisco_router]
         type = devconsole
         ip = 10.0.0.5
         real_ip = 172.10.0.3
         local_ip = 172.10.0.254
         virtual_ip = 10.0.0.5
         netmask = 255.255.255.0
         authtype = local
         template = devconsole.default
         description = CISCO router
```

Figure A-1: `onboard_server.ini` Device Entries With Templates Assigned

Note that the device with IPMI_1.5 type does not have a template.

Issues Affecting the Configuration of RSA-Type Service Processors

RSA I devices work differently from RSA II devices and recognize different commands. A RSA I type device may be made to work if the administrator copies the `talk_rsa_I.exp` file to a custom script named `talk_custom_N.exp`, modifies it as instructed in the script, and assigns the custom*N* type to the RSA I type device.

Some RSA II devices support management of event logs, sensors, and power through their command line interfaces and work with the `rsa.default template`. Some RSA II devices support only power commands through their command line interfaces, do not give access to event logs or sensors (although their web interfaces do provide event log and sensor access), and work only with the `rsa.limited.default` template, which only contains power commands. “To Find Out if An Existing Command Template Works With a New Device” on page 317 describes steps the OnBoard administrator can follow to find out whether one of the default RSA templates works, and if neither template works, to create a new template.

The onbdtemplate Utility

If the default command template that applies to the type of device being configured does not work, the administrator can use the `onbdtemplate` utility to test a new device against another command template. If needed, `onbdtemplate` can also be used to create a customized template to make command changes that might make it possible to communicate with a service processor whose firmware is slightly different from the tested version.

A template can be configured to keep repeating commands to achieve a goal such as reading output from multiple classes of sensors on an RSA II device or reading multiple event log files one by one until no more log files exist on an iLO-type service processor. Commands may be repeated until a string, such as “No more entries,” is returned. When commands are repeated, an escape sequence can be used to autoincrement the number in the command, which is needed, for example, when checking event log files.

The default editor used by `onbdtemplate` is `vi`. You can substitute `nano` for `vi` before invoking the `onbdtemplate` utility, as shown in the following screen example.

```
[root@OnBoard /] export EDITOR=/bin/nano
```

After being invoked, the `onbdtemplate` utility displays the action menu shown in the following screen example.

```
[root@OnBoard /] onbdtemplate
Please select action:

-View
 Edit
 New
 Copy
 Rename
 Delete
 Test
 Exit
```

Selecting “New” from the Action menu brings up an editor with a template file open for you to configure.

Selecting “View,” “Edit,” “Copy,” “Test,” or “Rename” from the Action menu brings up a menu of templates like the one shown in the following screen example

```
Please select template to view:

 drac.default
-rsa.default
 ilo.default
 rsa.limited.default
 devconsole.default
 Exit
```

If “Test” is selected, after the administrator selects a template, a list of devices that use the selected template appears, like the list shown in the following screen example

```
Select Service Processor to test against:

-rack1_ibm_e360_rsa_II
 rack2_ibm_e360_rsa_II
```

After the administrator selects a template and a device to test, a list of commands to test displays like the one shown in the following screen example.

```
Select a test to perform:

-Login and Native Command Interface
 Console Access
 Power On
 Power Status
 Power Cycle
 Reset
 Power Off
 System Event Log
 Clear Event Log
 Retrieve Sensors
 Test All
 Exit
```

Not all listed commands are supported on every device. If you select an unsupported command, an error message displays that lists the supported commands.

The first time you select any action to test, you are prompted to enter a username and password. If local authentication is specified for the device, enter the username and password that you entered to access the OnBoard. If another authentication method is specified for the device, use the appropriate username and password for the specified authentication method. The test command uses the same authentication and authorization processes that the OnBoard uses in its normal operation, as explained in under Chapter 1,

"Introduction" under on "Understanding Authentication on the OnBoard" on page 4" and "Understanding User and Group Configuration Options" on page 9.

See the following examples:

- The OnBoard uses local authentication, and the administrator logs into the OnBoard using the OnBoard username and password pair: `root/` *root_password*.
- The administrator tests the `rsa.default` command template on a server called rack1_ibm_e306_rsa, which is configured for RADIUS authentication with username scottb and password cycl123. The administrator must enter scottb and cycl123 to perform the test.
- The administrator tests the `rsa.default` command template on a server called rack2_ibm_e306_rsa, which is configured for LDAP authentication with username sburns and password 123cycl. The administrator must enter sburns and 123cyclto perform the test.
- The administrator tests the `rsa.default` command template on a server called rack3_ibm_e306_rsa, which is configured for local authentication. The administrator must enter the same username/password pair that was entered to access the OnBoard (root/*root_password*.) to perform the test.

Each set of commands may be tested in any order after the login test is performed. Errors are generated if a command is entered out of logical order; for example, if the Reset command is issued for a server that is not powered on. After any test you can return to the editor to make changes.

While using the editor to "Edit," "Copy," or create a "New" template, you can edit or delete fields and add comments. When the file is saved, error checking is performed. If an error is found, you are prompted either to enter the editor again to fix the error, or to discard the changes.

You cannot change templates whose name ends with `.default`. `onbdtemplate` warns about this restriction if you try to edit or rename these templates, and it requests confirmation before allowing you to create a new template with a `.default` suffix through the "New," "Rename," or "Copy" functions.

OnBoard Expect Scripts

The `Expect` scripts are located in the `/libexec/onboard` directory identified with the `.exp` suffix. The following table lists each of the defined device types with the name of the associated `Expect` script.

Table A-5: Default Device Types and Corresponding Expect Scripts

Device Type	Expect Script
iLO	`talk_ilo.exp`
RSA II	`talk_rsa_II.exp`
DRAC	`talk_drac.exp`
IPMI 1.5	`talk_ipmi_1.5.exp`
device console	`talk_devconsole.exp`

Three additional custom types (`custom1`, `custom2`, and `custom3`) allow OnBoard administrators to create up to three customized scripts. The following table shows the names of the `Expect` scripts associated with each of the custom types.

Table A-6: Custom Device Types and Corresponding Expect Scripts

Device Type	Expect Script
custom 1	`talk_custom1.exp`
custom 2	`talk_custom2.exp`
custom 3	`talk_custom3.exp`

By default, the `talk_custom`*N*`.exp` scripts contain warnings that they have not been configured along with some brief instructions on how to get them to work.

Note: Do not assign a `custom`*N* type to a device unless you have created a custom script with the same number in its name.

All `Expect` scripts reside in `/libexec/onboard`, as shown in the following listing.

```
[root@OnBoard /]  cd /libexec/onboard/
[root@OnBoard /]#  ls
bidi_login.exp          sensors.exp
talk_generic_ipmi.exp
common.exp            ssh_login.exp         talk_ilo.exp
gen_logrotate.sh      talk_custom1.exp      talk_ipmi_1.5.exp
local_log.exp         talk_custom2.exp      talk_rsa_I.exp
locking.exp           talk_custom3.exp      talk_rsa_II.exp
onbdauth              talk_devconsole.exp   template.exp
onbdunesc             talk_drac.exp
poll_sensors.sh       talk_generic.exp
```

The files fall into three categories:

- `talk_`*`devicetype`*`.exp` scripts are the `Expect` scripts for the various types of service processors.
- `talk_custom[1-3].exp` scripts are placeholders.

  The administrator can create a customized `Expect` script by copying, renaming, and modifying `talk_generic.exp`, `talk_generic_ipmi.exp` or one of the default `Expect` scripts. The administrator should set the file permissions to allow reading and execution by all users and writing by members of the admin group. The format of a custom `Expect` script's file name should be: `talk_custom`*`N`*`.exp`.

  Up to a total of three custom `Expect` scripts are supported. They must use the names of the placeholder custom scripts.

- `*_login.exp` scripts are special extension scripts that can be used to change how service processors are accessed from using `telnet` to another access method.
- Script templates are named `talk_generic.exp` and `talk_generic_ipmi.exp`.
- An example custom script (for the unsupported RSA I type), is named `talk_rsa_I.exp`.
- All other `Expect` scripts are used to handle tasks common to other Expect scripts, such as providing local logging services or processing the command templates.

Application Notes Related to Expect Scripts

Before configuring expect scripts, see the notes under `/usr/share/docs/OnBoard/Application_Notes/Service_Processor_Related`. The following table lists the subdirectories and describes the contents.

Table A-7: Expect Script Related Application Notes

Subdirectory name	Topic
APC	Managing APC IPDUs.
Alternate_Access	Using alternate means of communication with devices
Cisco	Managing devices running Cisco's IOS
Devconsoles	Managing devices that do not have service processors
Device_Clusters	Managing devices that in turn control other device
Grouping_Devices	Managing groups of devices
IBM	Managing IBM RSA I and RSA II service processors
IPMI 2.0	Taking advantage of IPMI v2.0 service processors
Native IP	Managing devices that require vendor supplied tools
Sun	Managing Sun ALOM and ILOM service processors

Table A-7: Expect Script Related Application Notes

Subdirectory name	Topic
Troubleshooting	More details about finding out what command template to use for a new device and creating a new template if needed.

After this document is finalized, more application notes may be created and installed in the `Service_Processor_Related` directory. For more details, see the `/usr/share/docs/OnBoard/Application_Notes/Service_Processor_Related/Readme.txt` file.

Also, before you start configuring new devices, check for additional application notes that may be posted after the product is released at `http://www.cyclades.com/support/downloads.php` under the product name "AlterPath OnBoard."

The following table lists the related topics and procedures under this section.

Example of Creating a Custom IPMI-Type Script	Page 332
SP/Device Expect Script Arguments	Page 333
SP/Device Expect Script Exit Codes	Page 335
To Create a Custom Expect Script	Page 336
To Create a Custom IPMI Expect Script	Page 333

Contact your Cyclades representative if you need additional support for creating a custom Expect script.

Example of Creating a Custom IPMI-Type Script

The OnBoard uses `ipmitool` commands to communicate with IPMI 1.5 type service processors. The OnBoard administrator can create a custom script to communicate with IPMI 2.0 type service processors in 1.5 compatibility mode or to use extra `ipmitool` arguments to support either OEM extensions or additional interfaces. To find a list of supported interfaces enter `ipmitool` with the `-h` option. To find a list of supported OEMs, enter `ipmitool` with the "`-o` *list*" argument.

▼ To Create a Custom IPMI Expect Script

1. Log into the OnBoard command line as root.
2. Go to the `/libexec/onboard` directory.
3. Copy the contents of `talk_generic_ipmi.exp` into the `talk_custom1.exp` file.
4. Follow the instructions in the file for how to get a list of `ipmitools` command options that you can use.
5. Save and quit the file.
6. Make sure the permissions are still 755.

SP/Device Expect Script Arguments

With one exception, each of the `Expect` scripts used to control access to a service processor takes exactly two arguments in the following format:

`talk_`*type*`.exp` *servername action*

The exception to the two-argument format occurs when the *action* is `spconsole`. When the second argument is `spconsole`, any other number of arguments may follow; all arguments entered after the `spconsole` action are collected into a single command to be executed in the device's native command interface.

`talk_`*type*`.exp` *servername* spconsole [*command1* | *command2* | ... *commandN*]

servername

The *servername* is the alias configured for the server or device on the OnBoard, for example, `rsa_us`. The script retrieves service processor/device specific information, such as the IP address, from the entry for the specified service processor/device, using the `llconf` program. This information is stored in the file `/etc/onboard_server.ini`, in the format known as ``INI file." For an example, see Table A-1, "`onboard_server.ini` Device Entries With Templates Assigned," on page 324.

action

The *action* specifies the action for the script to take. The actions are listed below. Not all service processor/device types implement all of the listed actions. For example, the iLO type does not have a sensors reading feature, so the sensors action is not supported for iLO-type servers. See "SP/Device Expect Script Exit Codes" on page 335 for the correct way to handle an unexpected action argument.

sensors

Asks the service processor for a sensor reading and display service processor sensor output on standard output

poweron

Asks the service processor to power up its server

poweroff

Asks the service processor to power down its server

powercycle

Asks the service processor to power cycle its server

powerstatus

Asks the service processor if its server is powered on

reset

Asks the service processor to reset its server

sel

Asks the service processor to retrieve the System Event Log and display the SEL contents on standard output

clearsel

Asks the service processor to clear the System Event Log

spconsole

The native command line of the service processor. Enters interactive pass-through mode. The script authenticates with the service processor, then connects the service processor output directly to its standard output and its standard input to the service processor input.

Note: `ssh` must be invoked with the `-t` option when this mode is used.

devconsole

Enters a console (also known as Device Console) session on a server whose service processor supports console access to the server or on a server or other device that supports device console access through its Ethernet port.

Note: `ssh` must be invoked with the `-t` option when this mode is used.

log_sensors

Retrieves sensor data in a standard format.

Note: `ssh` must be invoked with the `-t` option when this mode is used.

SP/Device Expect Script Exit Codes

Scripts that handle devices must end with one of the following exit codes.

Table A-8: Expect Script Exit Codes

Exit Code	Definition
0	Success
1	Unexpected output from service processor/device, or another error in a service processor protocol (such as timeout)
2	Bad command line (such as an incorrect number of arguments)
3	Action argument is not valid for the service processor/device type
4	Server or device given as first argument has not been configured

▼ *To Create a Custom Expect Script*

1. Access the command line of the OnBoard as an administrator.
2. Go to the `/libexec/onboard` directory.
3. Open one of the `talk_customN.exp` script files for editing.

Note: Use "talk_custom1.exp" for the first custom script, "talk_custom2.exp" for a second, and so on, up to a total of three scripts.

4. Copy the contents of a template or an existing script into the `talk_customN.exp` script file.
5. Edit the script as desired.
6. Save and quit the file.
7. Make sure the permissions are still 755.

Understanding Address Configuration for Connected Devices

As stated in "Preparing an Addressing Scheme" on page 55, the OnBoard administrator must plan and implement an IP addressing scheme to create a pool of private IP addresses to assign when configuring connected devices.

The following table lists the related topics the administrator needs to understand when doing the planning and implementation of the private IP addresses and provides links to where they are documented.

Table A-9: Tasks for Creating Addresses to Assign to Connected Devices (Sheet 1 of 3)

Task	Where Described
Private IP addresses must be defined by the creation of at least one *private subnet.* A private subnet must be created for each IP address range used by the connected devices.	• "Why Define Private Subnets?" on page 339 • "Configuring a Private Subnet" on page 340 • "Example 1: Private Subnet Configuration" on page 342 • "Example 2: Two Private Subnets and VPN Configuration" on page 345

Table A-9: Tasks for Creating Addresses to Assign to Connected Devices (Sheet 2 of 3)

Task	Where Described
Private subnet(s) should use IP addresses from one of the three IP address ranges reserved for use on internal networks.	• "Using Reserved IP Addresses for Private IP Addressing" on page 338
Even if virtual IP addresses are used (as described below), the planned real IP address for each device must be either configured manually as a static IP address or configured as a fixed address in the OnBoard's DHCP server `dhcp.conf` configuration file.	• "Options for Assigning IP Addresses to Connected Devices" on page 368
A *virtual network* should be created in the following cases: • To hide a device's private IP addresses from non-administrative users who are not configured for native IP access. • To simplify routing for PPTP VPN connections if IP addresses from different ranges have been previously configured for the devices' dedicated Ethernet ports, and the addresses cannot be changed.	• "Why Define Virtual (DNAT) Addresses?" on page 357 • To Configure IP Addresses From Multiple Ranges • "Example 3: Virtual Network With Two Private Subnets and VPN Configuration" on page 358

Table A-9: Tasks for Creating Addresses to Assign to Connected Devices (Sheet 3 of 3)

Task	Where Described
Any user who needs native IP access to the OnBoard needs to create a named VPN connection profile, then to create a VPN tunnel to the OnBoard before enabling native IP. The requirements for creating the VPN tunnel and the IP addresses to use vary depending on whether IPSec or PPTP is being used.	• "Routing Requirements for Native IP Access" on page 341 • "IPSec VPN Configuration for Example 2" on page 349 • "PPTP VPN Configuration for Example 2" on page 352 • "Enabling Native IP and Accessing a Device's Native Features Using Real IP Addresses for Example 2" on page 355 • "IPSec VPN Configuration for Example 3" on page 362 • "PPTP VPN Configuration for Example 3" on page 364 • "Enabling Native IP and Accessing a Device's Native Features Using Virtual Network Addresses for Example 3" on page 365

Using Reserved IP Addresses for Private IP Addressing

The OnBoard administrator should assign a private IP address to each connected device from one of the three IP Internet address ranges that are reserved for use on internal networks.

Table A-10: IP Address Ranges Reserved for Internal Network Addressing

Address Range	# of Networks/Class	Network Sizes
192.168.0.0—192.168.255.255	256/Class C	small (fewer than 200 hosts)
172.16.0.0—172.31.255.255	16/Class B	mid-sized
10.0.0.0—10.255.255.255	1/Class A	large

For recommendations about which ranges to use for various sizes of organizations and for avoiding address conflicts, see `http://www.rhebus.com/techinfo/iprange.htm#ip1`.

The number of IP address available on a network may be restricted by a subnet mask. For a simple example, the subnet mask 255.255.255.0 provides 256 IP addresses. The IP address ending with zero (0) is the network address, and the IP address ending with 255 is the broadcast address, leaving 254 addresses to assign to devices (from 1-254).

To specify a range of addresses on the AlterPath OnBoard supply the network address and a subnet mask, in either of these two formats: 192.168.0.0 and 255.255.255.0 or 192.168.0.0/24.

Why Define Private Subnets?

At least one *private subnet* must be defined on the OnBoard for the following purposes:

- To define a private OnBoard address for the OnBoard and connected devices to use when communicating.
- To enable communications between remote user's workstations on the Internet or local user's on the same LAN and connected devices on the private management network, via the OnBoard's Native IP access facility.

The private Ethernet ports are accessed through the `priv0` interface on the OnBoard, which interacts with connected devices through an internal switch.

The OnBoard attempts to reach a device that does not have a private subnet assigned by attempting to contact it through the OnBoard's default route. Therefore, unless the OnBoard administrator defines a private subnet and assigns it to each device, the device cannot be reached unless the device is on the public side of the OnBoard. In almost all cases, devices are on the private side of the OnBoard and therefore they are unreachable without a private subnet.

The following should be kept in mind when planning the addressing scheme:

- When the connected devices' addresses are all within the same range, only one private subnet is required.
- The administrator should assign IP addresses to all service processors from the same block of addresses, if possible, to make it possible to administer the IP addresses using only a single private subnet.

- When the connected devices' addresses are already configured in multiple ranges and the addresses cannot be changed, or when for some other reason, connected devices must have addresses in multiple address ranges, multiple private subnets must be created. (To simplify routing for PPTP VPN connections, multiple private subnets may also require configuration of a virtual network, as described in "Why Define Virtual (DNAT) Addresses?" on page 357.)
- The `priv0` interface, which is used for all the private Ethernet ports, is not assigned an IP address unless a private subnet is configured.

  The following screen example shows the default `ifconfig` output for `priv0`., which shows no IP address.

```
priv0     Link encap:Ethernet  HWaddr 00:60:2E:BB:AA:AA
          UP BROADCAST RUNNING MULTICAST   MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
           TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
          Base address:0xe000
```

The OnBoard administrator must define IP address or addresses for `priv0` by defining private subnet(s). When multiple private subnets exist, their IP addresses are assigned to aliases of `priv0`, such as `priv0:sub1` and `priv0:sub2`.

Configuring a Private Subnet

An administrator configures a private subnet by doing the following:

- Defining a range of IP addresses which administrators can assign to devices that are connected to the OnBoard's private ports
- Designating one of the IP addresses within the specified range to be used by the OnBoard. The OnBoard-side address must be used by users when creating a IPSec VPN connection to enable native IP access.

The OnBoard uses the specified information to create a route to the private subnet.

The range of IP addresses is derived from the information shown in the following table, which the administrator supplies to define a private subnet:

Table A-11: Values for Configuring a Private Subnet

Field	Definition
Private subnet name	Any meaningful name chosen by the administrator, such as privnet1.
OnBoard side IP address	Devices use this address when communicating with the OnBoard. The OnBoard uses this address when communicating with devices. This address must be within the private subnet's IP address range.
Subnet mask	Defines the range of addresses available on the private subnet.

The system derives the range of addresses that can be used for talking to devices by using the network portion of the OnBoard's IP address and from the private subnet netmask that the administrator specified.

When configuring a device, the administrator assigns the private subnet to the device and assigns an IP address within the range specified for the private subnet. The OnBoard uses the device's IP address when talking to a device, and devices use the OnBoard's assigned address when talking the OnBoard.

When a private subnet is configured, the private subnet name is assigned to the priv0 interface in the form `priv0:`*private_subnet-name* along with the IP address assigned to the OnBoard in the form `inet addr:` *OnBoardIPaddr*. If multiple private subnets are configured, multiple `priv0:`*private_subnet-name* interfaces exist, each with its administratively-configured private subnet IP address for the OnBoard. See the following examples for sample `ifconfig` output:

- "Example 1: Private Subnet Configuration" on page 342
- "Example 2: Two Private Subnets and VPN Configuration" on page 345

Routing Requirements for Native IP Access

As documented in the *AlterPath OnBoard User's Guide*, users who are authorized for native IP access need to create a IPSec or PPTP VPN connection before gaining native IP access.

Any routes needed for IPSec VPN can be configured as part of the IPSec connection by setting the “nexthop” to the IP address of the desired network or host route and setting the boot action to “Add and route.”

Any route(s) needed for PPTP must be configured manually.

See “IPSec VPN Configuration for Example 2” on page 349, “PPTP VPN Configuration for Example 2” on page 352, “IPSec VPN Configuration for Example 3” on page 362, and “PPTP VPN Configuration for Example 3” on page 364, which discuss routing requirements for the two types of VPN connections and show example routes.

Example 1: Private Subnet Configuration

Figure A-2 shows a private subnet configuration example.

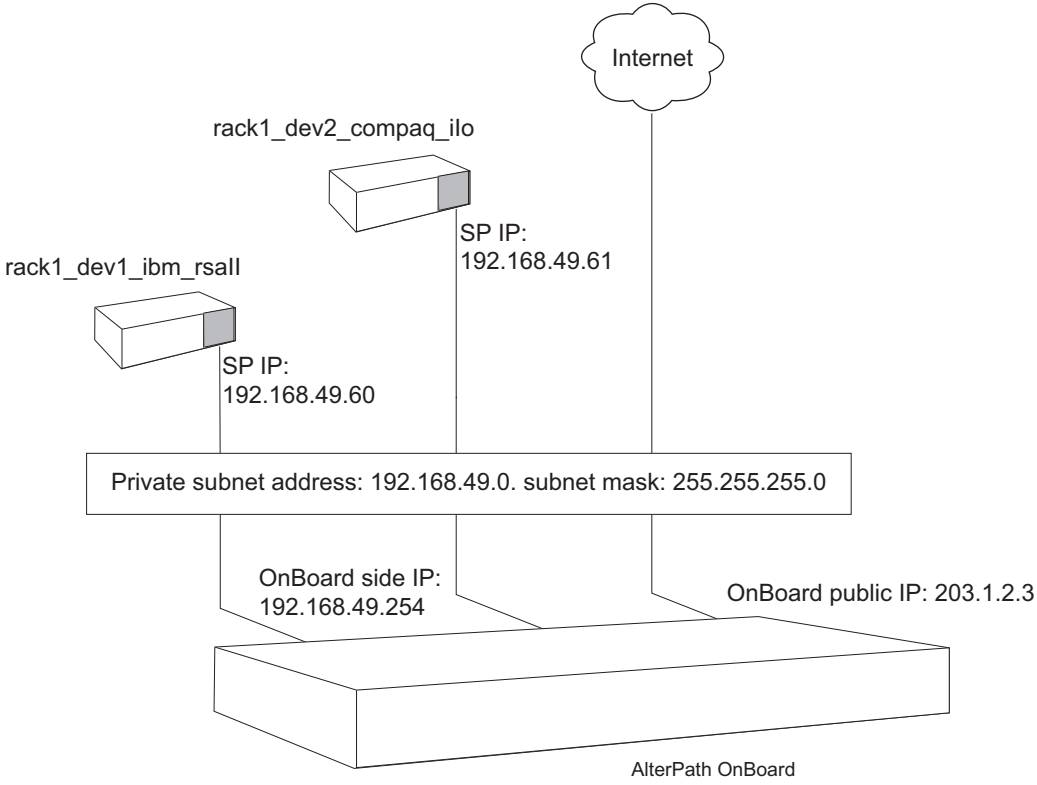


Figure A-2: Example 1: Private Subnet

In Figure A-2, two devices are connected to the OnBoard. The public Ethernet port on the OnBoard has a public IP address of 203.1.2.3. The administrator plans to assign the following:

- Two private IP addresses within the 192.168.49.0 network range to the devices on the OnBoard's private network: 192.168.49.60 and 192.168.49.61,
- A third private IP address within the same range to the OnBoard: 192.168.49.254.

Figure A-3 shows the values the administrative user would enter in the Web Manager to configure the private subnet shown in Figure A-2.

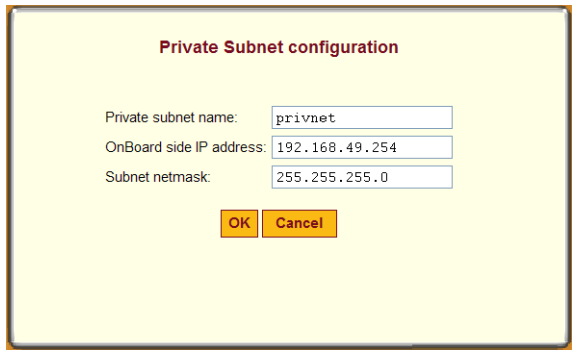


Figure A-3: Private Subnet Configuration Example

Figure A-3 shows the following values entered in the dialog that appears when the "Add Subnet" button is clicked on the Network → Private subnets screen:

- Private subnet name: privnet
- OnBoard side IP address: 192.168.49.254
- Subnet netmask: 255.255.255.0.

The private subnet address derived from the configuration in Figure A-3 is 192.168.49.0. For this network IP address, the conventional broadcast address is 192.168.49.255. Because the OnBoard's address is 192.168.49.254, the administrator can assign any remaining IP address between 192.168.49.1 and 192.168.49.253 when configuring a connected device.

The following figure shows these values: Private subnet "privnet," and Device IP address 192.168.49.61 assigned to the device rack1_dev2_compaq_ilo on

the Web Manager → Config Devices screen, as part of the implementation of the configuration shown in Figure A-2.

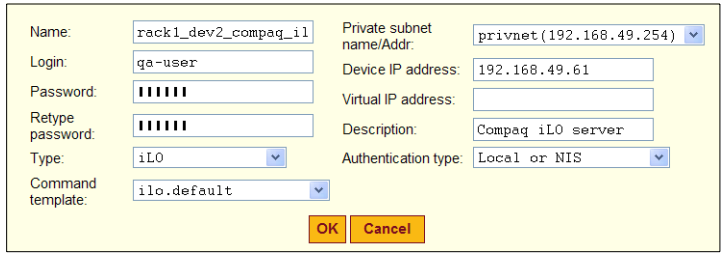


Figure A-4: Example 1: Device Configuration Example

As shown in the following screen example, the new private subnet name and the OnBoard-side IP address and subnet mask from Figure A-3 are assigned to the `priv0` interface.

```
priv0:privnet Link encap:Ethernet  HWaddr 00:60:2E:BB:AA:AA
          inet addr:192.168.49.254  Bcast:192.168.49.255
          Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          Base address:0xe000
```

Figure A-5: `ifconfig` Output Showing a `priv0` Private Subnet Alias

Example 2: Two Private Subnets and VPN Configuration

Figure A-6 shows an example with four devices. Two subnets must be created because the devices “sp3” and “sp4” have IP addresses that cannot be changed, and their addresses are not in the same network range as the other two devices. Configuration details follow, including how to set up VPN connections.

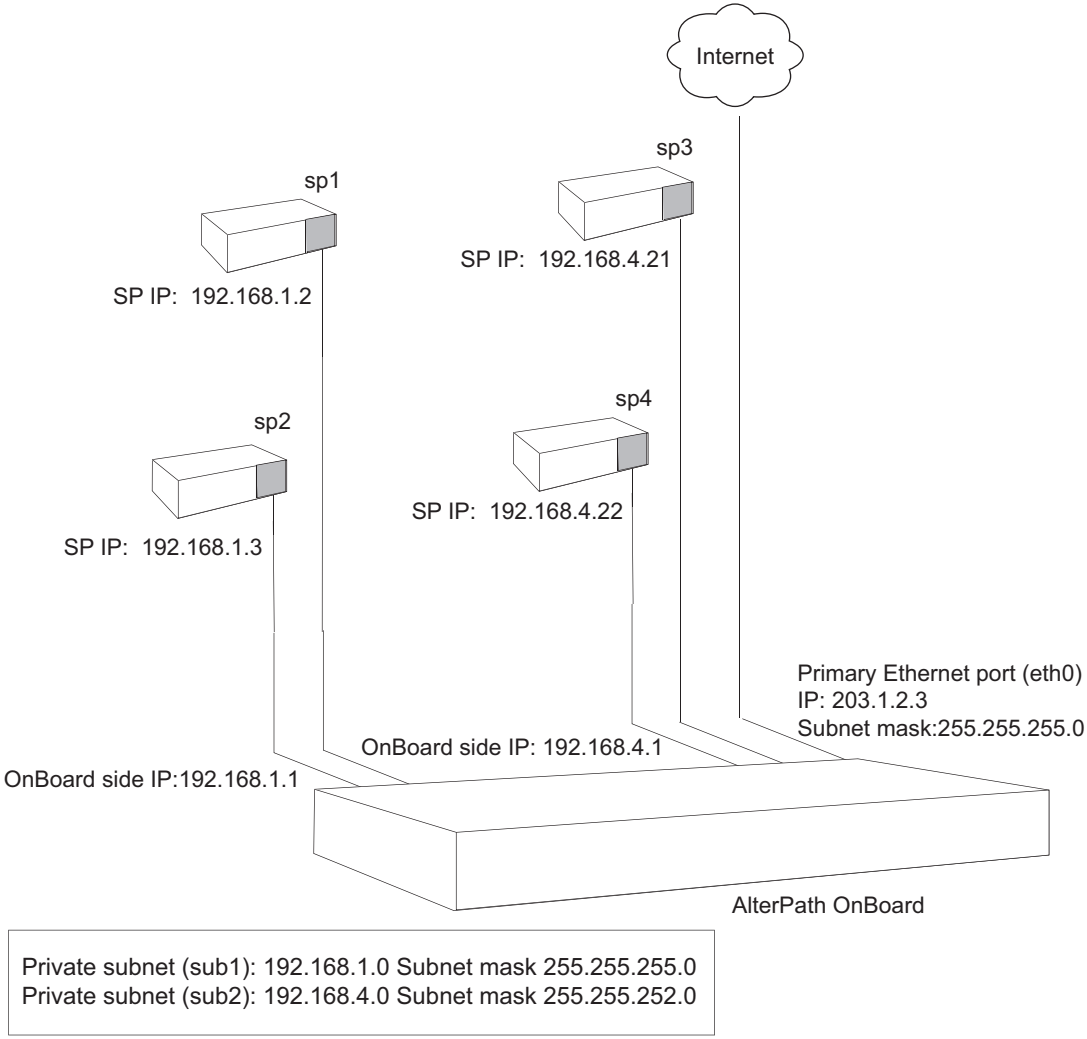


Figure A-6: Example 2: Two Private Subnets

Two Private Subnets and User Configuration for Example 2

Configuration of the private subnets shown in Figure A-6 is described in the following bulleted list:

- The primary Ethernet port is configured with IP address 203.1.2.3 and subnet mask 255.255.255.0.
- A default route is automatically created using a gateway IP 203.1.2.254, which the administrator assigned when configuring the primary Ethernet port.
- Private subnets are configured as aliases to `priv0` by defining the OnBoard side IP addresses and netmasks shown in Figure A-6 and listed here:
  - Private subnet “sub1”
  - OnBoard side IP address: 192.168.1.1
  - Subnet mask: 255.255.255.0

  The above values define a range between 197.168.1.0 and 192.168.1.255 = 256 addresses, of which 254 are usable.
  - Private subnet “sub2”
  - OnBoard side IP address: 192.168.4.1
  - Subnet mask: 255.255.252.0

  The above values define a range between 197.168.4.0 and 192.168.7.255 = 1054 addresses, of which 1022 are usable. This subnet is defined with this address range because device “sp3” and “sp4” have previously been assigned IP addresses within this range, and the addresses cannot be changed.

  The following figure shows the values entered on the Web Manager Network → Private subnet screen to implement the private subnets in this example.

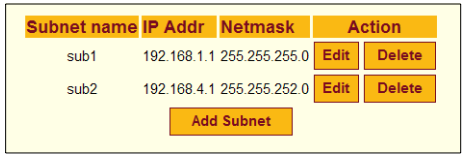


Figure A-7: Example 2: Values for Configuring Two Subnets on the Network → Private Subnet Screen

As shown in the example output from the `ifconfig` command on the OnBoard in the following figure, both private subnet names are assigned as aliases to the `priv0` interface, and the OnBoard-side IP addresses and subnet masks from Figure A-7 are assigned to the each alias.:

```
priv0:sub1 Link encap:Ethernet  HWaddr 00:60:2E:BB:AA:AA
           inet addr:192.168.1.1  Bcast:192.168.0.255
           Mask:255.255.255.0
           UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
           Base address:0xe000
priv0:sub2 Link encap:Ethernet  HWaddr 00:60:2E:BB:AA:AA
           inet addr:192.168.4.1  Bcast:172.10.0.255
           Mask:255.255.252.0
           UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
           Base address:0xe000
```

Figure A-8: `ifconfig` Output With `priv0` Aliases for Two Private Subnets

The configuration of the devices shown in Figure A-6 is described in the following bulleted list:

- "sp1" is on private subnet "sub1," so it needs an IP address in the range 192.168.1—192.168.1.255: 192.168.1.2.
- "sp2" is also on private subnet "sub1," so its IP address in the same range: 192.168.1.3.
- "sp3" is on private subnet "sub2." It has previously been assigned the IP address 192.168.4.21, which cannot be changed.
- "sp4" is also on private subnet "sub2." It has previously been assigned IP address 192.168.4.22 and its address cannot be changed either.

  The following figure shows the values specified on the Web Manager Config → Devices: Add new devices dialog to specify the private subnet, and the device IP for "sp1,", "sp2," "sp3," and "sp4."

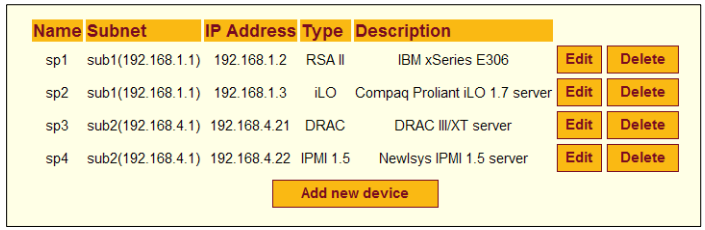


Figure A-9: Example 2: Four Devices Configured on the Web Manager Config → Devices Screen

The OnBoard administrator must do the following to configure the user to be able to create the VPN tunnel:

- Make sure the user who needs the VPN access has an account that is authorized for native IP access to the devices.

  The following screen example shows the configuration information entered on the Config → Users and groups: Device Access dialog to authorize a user name “allSPs” for native IP access to all four devices in this example.

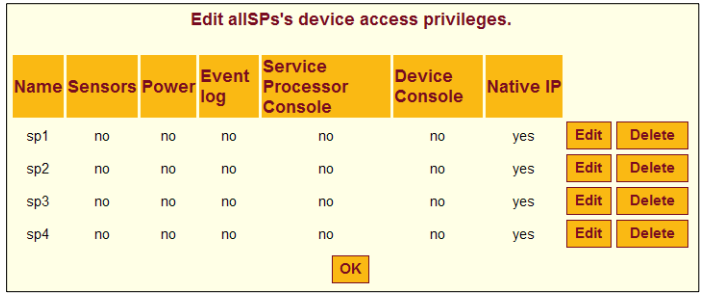


Figure A-10: Example 2: Configuration for a User Account Authorized for Native IP Access to All Configured Devices

A VPN connection must exist before a user can access native IP management features on a device. The following table lists examples that show how the VPN connections can be created using IPSec or PPTP. For these examples, the IP address of the user's workstation is `12.34.56.78`.

Table A-12: Examples for Creating IPSec and PPTP VPN Connections for Example 2

Type of VPN	Where Documented
Create an IPSec VPN connection	"IPSec VPN Configuration for Example 2" on page 349
Create a PPTP VPN connection	"PPTP VPN Configuration for Example 2" on page 352

IPSec VPN Configuration for Example 2

After the private subnets, device, and user account configuration in "Two Private Subnets and User Configuration for Example 2" on page 346 is completed, a VPN connection must be created. This example shows the configuration steps that must be performed by the OnBoard administrator and by a user on a remote workstation for enabling two IPSec VPN connections. One connection supports the IPSec VPN tunnel from the user's workstation to "sp1" and "sp2." The second connection supports the IPSec VPN tunnel to "sp3" and "sp4."

The OnBoard administrator must also do the following to enable an IPSec client to access the private subnets where the devices reside:

- Make sure that the IPSec service is enabled on the OnBoard.
- Obtain the IP address of the user's workstation and use it to create two named IPSec connections ("connSub1" and "connSub2") with the following values specified:
  - Left ID: @onboard
  - Left IP address: 203.1.2.3 (must be one of the OnBoard's public IP addresses)
  - Left nexthop: leave blank if the user's workstation and the OnBoard are able to exchange packets.

Note: The user can test whether the user's workstation can access the OnBoard by entering the OnBoard's public IP address in a browser to try to bring up the Web Manager.

- When configuring “connSub1” for access to sub1: Left subnet: 192.168.1.0/24
- When configuring “connSub2” for access to sub2: Left subnet: 192.168.4.0/22
- Right ID: @workstation
- Right IP address: the IP address of the user’s workstation: 12.34.56.78
- Right nexthop: leave blank if the user’s workstation and the OnBoard are able to exchange packets.
- Right subnet: leave blank

The other IPSec configuration parameters (such as Authentication protocol and Boot action) would be determined by the site’s policy, equipment compatibility, and site routing requirements.

Note: In some circumstances (for example, if packets are being blocked by a firewall on the client’s default gateway), the user’s workstation and the OnBoard are not going to be able to exchange packets. Setting one or both of the Right and Left nexthop parameters to the IP address of a host route and selecting “Add and route” as the boot action may be needed to create a route that allows the two endpoints to communicate.

The following screen example shows the configuration on the Web Manager Network → VPN connections: IPSec Add new connection dialog for a connection named “connSub1,” with the values specified from the above list. Configuration of “connSub2” would be similar, with a different “Connection name” and “Left subnet values.”

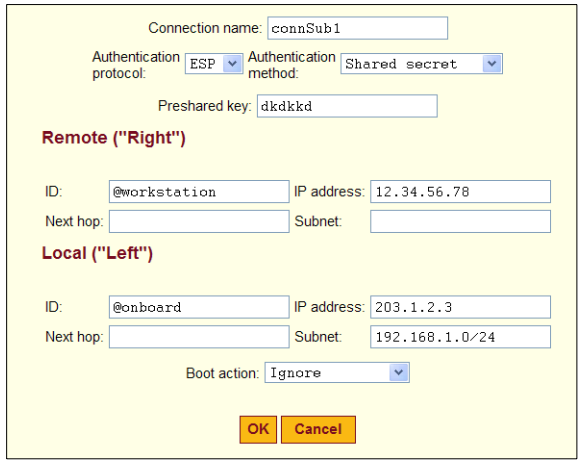


Figure A-11: Example 2: IPSec Connection Configuration for Access to sub1 Private Subnet and "sp1" and "sp2" Devices

In addition, the OnBoard administrator must do the following to enable the IPSec client to access the subnets where the devices reside.:

- Give the user a copy of the parameters used to configure the IPSec connection profiles on the OnBoard.

  The OnBoard administrator can send a copy of the relevant portions of the `ipsec.conf` file after the changes are saved and applied in the Web Manager for the user to insert into the `ipsec.conf` file on the user's workstation.

The authorized user must do the following to enable the IPSec client running on the user's workstation to bring up the VPN tunnel to access the subnets where the devices reside, and then to access the native IP features on the devices.

- Use the same values used by the OnBoard administrator to create an IPSec VPN connection profile on the user's workstation.

  If the OnBoard administrator sends the relevant portions of the `ipsec.conf` file from the OnBoard's IPSec configuration, use it to replace the same section in the workstation's `ipsec.conf` file.

- Bring up the IPSec VPN tunnel.

  Depending on the platform and IPSec client being used, the user may use a GUI or execute the `ipsec auto -up` command. IPSec automatically

creates the routes needed to get packets flowing through the tunnel, so neither the user nor the administrator need to create routes to support IPSec access to devices.

- Enable native IP and access the device's native features.

  See "Enabling Native IP and Accessing a Device's Native Features Using Real IP Addresses for Example 2" on page 355.

PPTP VPN Configuration for Example 2

After the private subnets, device, and user account configuration in "Two Private Subnets and User Configuration for Example 2" on page 346 is completed, a VPN connection must be created. This example shows the configuration steps that must be performed by the OnBoard administrator and by a user on a remote workstation for setting up an PPTP VPN connection[1] that would enable the authorized user "allSps" to access "sp1," "sp2," "sp3," and "sp4."

The OnBoard administrator must do the following to enable the PPTP client:

- Make sure that the PPTP service is enabled.
- Configure PPTP on the OnBoard.

  The following screen example shows an example PPTP configuration on the Network → VPN connections screen.

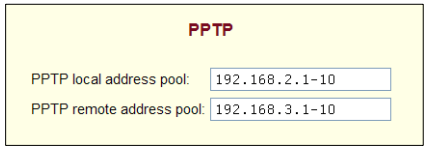


Figure A-12:PPTP VPN Configuration Example: Address Pools

Figure A-12 shows the following address pools:

- PPTP local address pool: 192.168.2.1-10
- PPTP remote address pool: 192.168.3.1-10

1. A VPN connection must exist before a user can access native IP management features on a device.

Note: The address pools' IP addresses can be assigned arbitrarily. Make sure that none of the addresses assigned here are being used elsewhere on your network.

- Make sure the following are done for the user who needs the PPTP VPN access:
  - The user's account is authorized for native IP access to "sp1," "sp2," "sp3," and "sp4" as shown in Figure A-10.
  - The user's account is configured for PPTP access to the OnBoard as shown in Figure A-13.

    The following figure shows an example PPTP configuration on the Config → Users and groups screen.

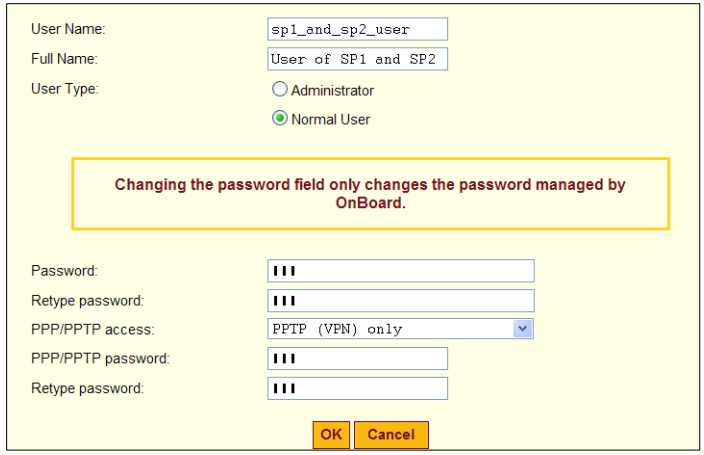


Figure A-13:PPTP User Configuration Example

Note: The user can be configured for PPTP alone or for both PPP/PPTP.

  - The user's workstation is running PPTP client software.
  - The user has the PPTP password if it is different from the password that authenticates the user for access to the OnBoard.

The authorized user must do the following:

- Make sure the user's workstation can exchange packets with the OnBoard.

  The user can test whether the user's workstation can access the OnBoard by entering the OnBoard's public IP address in a browser to try to bring up the Web Manager.

- If a network or host route is needed to enable communications with the OnBoard, configure the route.
- Use the PPTP client on the workstation to create the PPTP VPN connection profile, entering the following:
  - PPTP server address = OnBoard public IP address (203.1.2.3)
  - Username = OnBoard user name, in this example: allSPs
  - Password = PPTP password
- Create the PPTP VPN connection.
- Enter the `ifconfig` or `ipconfig` command on the command line of the user's workstation to discover the IP address assigned to the OnBoard's end of the PPTP VPN tunnel.

  When the PPTP tunnel is being activated, the OnBoard chooses an IP address from each of the address pools for the endpoints of the PPTP link. The client's end of the point-to-point link receives an address from the remote address pool, and the OnBoard receives an address from the local address pool. Usually the first connection obtains the first address from each pool, so the client would be `192.168.3.1` and the OnBoard would be `192.168.2.1`.

- Enter the OnBoard's PPTP-assigned address either in a browser or with `ssh` on the command line to access the OnBoard. In this example the address would be `192.168.2.1`.
- Create a static route to inform the workstation that the devices to be contacted are at the other end of the point-to-point link.
- In this example, to communicate with "sp1" and "sp2," a route would needed to "sub1," which has the network IP address `192.168.1.0` as shown below:

```
route add -net 192.168.1.0 mask 255.255.255.0 via 192.168.2.1
```

- To communicate with “sp3” and “sp4,” a route would needed to “sub2,” which has the network IP address `192.168.4.0` as shown below:

```
route add -net 192.168.4.0 mask 255.255.255.0 via 192.168.2.1
```

- Enable native IP and access the device’s native features.

  See “Enabling Native IP and Accessing a Device’s Native Features Using Real IP Addresses for Example 2” on page 355.

Enabling Native IP and Accessing a Device’s Native Features Using Real IP Addresses for Example 2

After creating the VPN tunnel as described in “IPSec VPN Configuration for Example 2” on page 349 or “PPTP VPN Configuration for Example 2” on page 352, the user uses the OnBoard side IP address configured for the appropriate private subnet to access the OnBoard, and then enables Native IP access to the desired device.

Enabling Native IP Access

In this example, to enable native IP access on “sp1” or “sp2” on “sub1,” the user would enter the OnBoard side IP address for “sub1” (which is `192.168.1.1`) in one of the two following ways:

- In a browser on the user’s workstation, the user would do the following:
  - Bring up the Web Manager using `http://192.168.1.1`.
  - Chose the “Devices” left menu option.
  - Select “sp1” or “sp2.”
  - Click Enable Native IP access
- On the user’s workstation’s command line, the user would do the following:
  - Use `ssh` to connect to the OnBoard’s console and to access the `rmenush` menu in one of the following ways:

    `ssh` *username*`:192.168.1.1`

    `ssh -t` *username*`:@192.168.1.1 menu`
  - Select “Access Devices” from the menu.
  - Select either “sp1” or “sp2” from the devices menu.

- Select “Enable native IP” from the list of management actions the user is authorized to perform on the device.

OR

- Use `ssh` to execute the `nativeipon` command directly using the device alias:

  `ssh` *username*`:`*device_alias*`@192.168.1.1 nativeipon`

Accessing Native Features for Example 2

After enabling native IP access, the user can access one of the desired native features that may be available on the device, including:

- A native web application, which may be accessed in one of the following ways:
  - In the Web Manager on the OnBoard, clicking the “Go to native web interface” link on the Access Devices screen.
  - On the user’s workstation, entering the IP address or DNS-resolvable name of the device in a browser.
  - On the user’s workstation, on the command line, entering the `ssh` command with the name/alias of the device along with the IP address of the OnBoard side address for the subnet where the device resides.

    For example, see the following `ssh` command line entered by the user named “allSPs” to access “sp2” on the private subnet whose OnBoard side IP address is `192.168.1.1`.

    ```
    ssh -t allSPs:sp2@192.168.1.1
    ```

- A management application, which may be accessed in one of the following ways, depending whether the application is a client on the user’s workstation or resides on the service processor:
  - If the management application resides on the user's workstation, by bringing it up from there.
  - If the management application resides on the service processor, and is an executable that can be invoked on the command line, by accessing the service processor’s console first in one of the following two ways:
    - Invoking `ssh` with the `spconsole` command in the following format

    ```
    ssh -t allSPs:sp2@192.168.1.1 spconsole
    ```

OR

- In the Web Manager on the OnBoard, clicking the “Service Processor Console” link on the Access Devices screen.

AND

- Bringing the management application up from the service processor’s command line.

- The console of the server on which the service processor resides, in one of the following two ways:.
  - Invoking `ssh` with the `devconsole` command in the following format

    ```
    ssh -t allSPs:sp2@192.168.1.1 devconsole
    ```

    OR

  - In the Web Manager on the OnBoard, clicking the “Device Console” link on the Access Devices screen.

Why Define Virtual (DNAT) Addresses?

A virtual network based on Destination Network Address Translation (DNAT) should be defined in the following cases:

- To hide the addresses of the connected devices from users by the use of *virtual IP addresses*.

Caution! When an authorized user has service processor access, device console access, or native IP access, there is no way to prevent that user from seeing the IP address of the device while the user is connected.

  It is possible and desirable to hide devices’ real IP addresses from users who are authorized to access all other device management capabilities other than native IP, service processor console, or device console.

- When multiple *private subnets* must be supported, and you do not want to require authorized users to configure routes to each network.

  For example, if three connected devices have addresses 192.168.0.1, 10.0.25, and 17.10.11.12, three private subnets could be defined. A virtual network would map the IP addresses from the three private subnets to virtual IP addresses in the same virtual network range.

The following table describes the information that defines a virtual network.

Table A-13: Information Defining a Virtual (DNAT) Network

Field	Description
Address	IP address to assign to the OnBoard from the virtual network address range. For example, if the virtual IP address of the network is 10.0.0.0, 10.0.0.254 would be a valid IP address that could be assigned to the OnBoard. The administrator would then have all the other addresses to assign to devices, except for 10.0.0.0 and 10.0.0.255.
Netmask	Netmask (which is used in combination with the network address portion of the "Address" above to define the address range of the virtual network.

Note: Some service processors do not work with virtual network (DNAT) addresses.

Example 3: Virtual Network With Two Private Subnets and VPN Configuration

This example adds to the configuration of two private subnets with four devices shown in Figure A-9 by configuring a virtual network, which has the following benefits:

- It simplifies routing for PPTP VPN users.
- It hides IP addresses from users who are authorized only for one of the following types of device management actions:
  - Power commands
  - Sensor commands
  - System event log commands

As stated elsewhere, users who have the following types of access to a device cannot be prevented from seeing the real IP address of the device:

- Native IP
- Device console
- Service processor console

The following figure (Figure A-14) shows the same configuration as Figure A-6, but with the addition of virtual IP addresses.

Figure A-14 shows an example of virtual network configuration that enables virtual addresses to be assigned to connected devices and to the OnBoard. The administrator plans to assign virtual IP addresses in the 172.20.0.1 range to hide the real private subnet IP addresses.

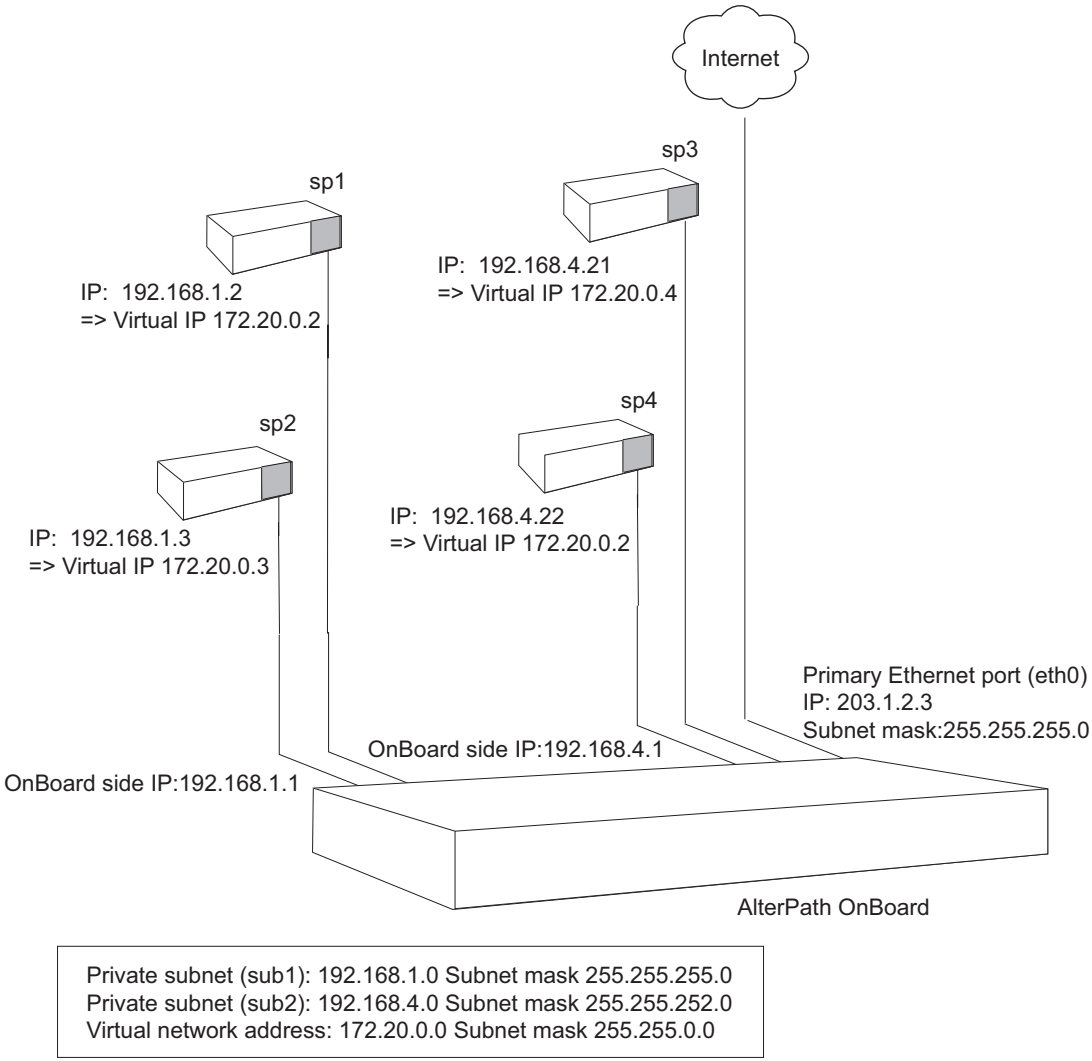


Figure A-14: Example 3: Virtual Network Configuration

Note: "sp4" in Figure A-14 is one of the service processors that do not work with virtual network (DNAT) addresses.

Virtual Network and Device Configuration for Example 3

To hide the real addresses of the devices from users according to the ongoing example, the OnBoard administrator would need to do the following configuration:

- Assign the device named "sp1" a virtual IP of 172.20.0.2.
- Assign the device named "sp2" a virtual IP of 172.20.0.3.
- Assign the device named "sp3" a virtual IP of 172.20.0.4.
- The device named "sp4" with IP 192.168.4.22 does not work with virtual network (DNAT) addressing, so it cannot be contacted using a virtual IP address. Therefore, the administrator does not assign "sp4" a virtual IP.

To make it possible to assign the virtual addresses shown in Figure A-14, the OnBoard administrator needs to configure a virtual network with the following values:

- Address: A virtual address from the desired virtual address range to assign to the OnBoard, in this case: 172.20.0.1
- Netmask: 255.255.0.0

The following figure shows the desired values entered on the Web Manager Network → Private subnet: Add Subnet screen.

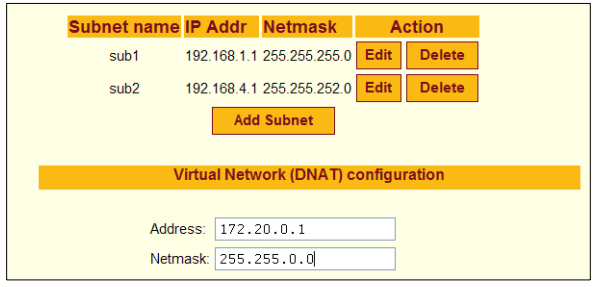


Figure A-15: Example Values for Configuring Two Private Subnets With a Virtual Network

Finally, the administrator also must configure the devices that support virtual addressing with a virtual address from the 172.20.0.0 virtual network IP range. For example, the following figure shows the virtual IP address 172.20.0.2 assigned to the device “sp1” on the Web Manager Config Devices screen to implement the configuration shown in Figure A-14.

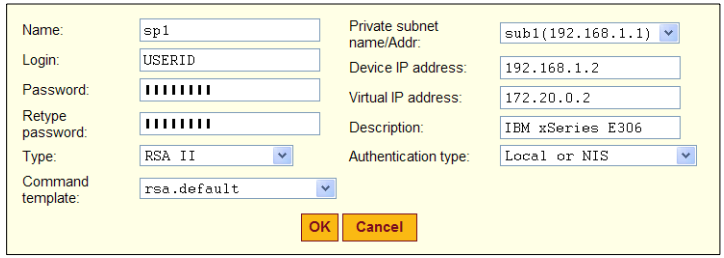


Figure A-16: Example 1: Device Configuration Example

Figure A-17 shows the entries on the Devices screen for the devices shown in Figure A-14. Note that the IP addresses for “sp1,” “sp2,” and “sp3” are hidden, and the user can only see the devices’ virtual IP addresses. Because “sp4” does not work with virtual IPs and no virtual IP was configured for “sp4,” the user sees “sp4”’s real IP address.

Service Processor/Device	Feature(s)
Name: sp1 **IP:** 172.20.0.2 **Description:** IBM xSeries E306	Service Processor Console Device Console Power Reset Sensors Event Log Native IP: Not available
Name: sp2 **IP:** 172.20.0.3 **Description:** Compaq Proliant iLO 1.7 server	Service Processor Console Device Console Power Reset Sensors Event Log Native IP: Not available
Name: sp3 **IP:** 172.20.0.3 **Description:** DRAC III/XT server	Service Processor Console Device Console Power Reset Sensors Event Log Native IP: Not available
Name: sp4 **IP:** 192.168.4.22 **Description:** Newisys IPMI 1.5 server	Service Processor Console Device Console Power Reset Sensors Event Log Native IP: Not available

Figure A-17: Access → Devices Screen With Virtual IP Addresses

IPSec VPN Configuration for Example 3

After the private subnets, device, and user account configuration in “Virtual Network and Device Configuration for Example 3” on page 360 is completed, a VPN connection must be created. With a virtual network, only one IPSec VPN connection must be configured to create the IPSec VPN tunnel from the user’s workstation to “sp1,” “sp2,” and “sp3,” which are on both private subnets in example 3.

Configuration of “connSub2” would be still be needed as in “IPSec VPN Configuration for Example 2” on page 349, because the only way a user could contact “sp4” would be through the private subnet IP.

The values used for enabling an IPSec VPN connection are the same as in “IPSec VPN Configuration for Example 2” on page 349, except the OnBoard administrator must configure the Left subnet: by entering 172.20.4.0/22 to configure the connection to the virtual network.

The following screen example shows the configuration on the Web Manager Network → VPN connections: IPSec Add new connection dialog for a connection named “connVirt,” with the values specified from the previous paragraph.

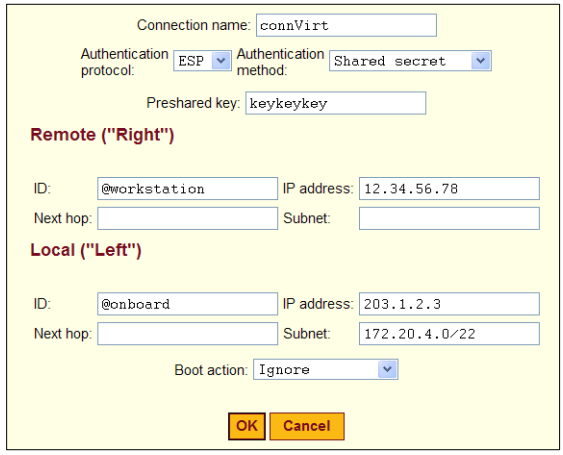


Figure A-18: Example 3: IPSec Connection Configuration for Access to sub1 Private Subnet and “sp1” and “sp2” Devices

As in the earlier example, the OnBoard administrator must do the following to enable the IPSec client to access the subnets where the devices reside:

- Give the user a copy of the parameters used to configure the IPSec connection profiles on the OnBoard.

  The OnBoard administrator can send a copy of the relevant portions of the `ipsec.conf` file after the changes are saved and applied in the Web Manager for the user to insert into the `ipsec.conf` file on the user’s workstation.

The authorized user must do the following to enable the IPSec client running on the user's workstation to bring up the VPN tunnel to access the subnets where the devices reside, and then to access the native IP features on the devices.

- Use the same values used by the OnBoard administrator to create an IPSec VPN connection profile on the user's workstation.

  If the OnBoard administrator sends the relevant portions of the `ipsec.conf` file from the OnBoard's IPSec configuration, use it to replace the same section in the workstation's `ipsec.conf` file.

- Bring up the IPSec VPN tunnel. For accessing "sp1," "sp2," or "sp3," the user can use the connVirt connection profile. For accessing "sp4", the user uses the "connSub2" connection profile.

Enabling native IP and accessing the device's native features is the same as described under "Enabling Native IP and Accessing a Device's Native Features Using Real IP Addresses for Example 2" on page 355.

PPTP VPN Configuration for Example 3

After the private subnets, device, and user account configuration in "Virtual Network and Device Configuration for Example 3" on page 360 is completed, a VPN connection profile must be defined to create a VPN tunnel to the virtual network.

The steps used for enabling a PPTP VPN connection to the virtual network are the same as in "PPTP VPN Configuration for Example 2" on page 352, except that, after creating the PPTP VPN tunnel, the user must create the static route differently to access the virtual network.

This first set of bullets are a review of the steps for obtaining the PPTP address assigned to the OnBoard:

- Enter the `ifconfig` or `ipconfig` command on the command line of the user's workstation to discover the IP address assigned to the OnBoard's end of the PPTP VPN tunnel.
- Enter the OnBoard's PPTP-assigned address either in a browser or with `ssh` on the command line to access the OnBoard. In this example the address is `192.168.2.1`.

The next bulleted items shows how to create an appropriate route to the virtual network.

- Create a static route to inform the workstation that the devices to be contacted are at the other end of the point-to-point link.

  In this example, to communicate with “sp1,” “sp2,” and “sp3,” a route would needed to the virtual network whose IP address is `172.20.0.0` as shown below:

```
route add -net 172.20.0.0 mask 255.255.0.0 via 192.168.2.1
```

  To communicate with “sp4”, because it cannot be contacted through a virtual network IP address, the same route mentioned in “PPTP VPN Configuration for Example 2” on page 352 would be needed to “sub2,” which has the network IP address 192.168.4.1 as shown below:

```
route add -net 192.168.4.1 mask 255.255.252.0 via 192.168.2.1
```

- Enable native IP and access the device’s native features.

Enabling native IP and accessing the device’s native features is the same as described under “Enabling Native IP and Accessing a Device’s Native Features Using Real IP Addresses for Example 2” on page 355.

Enabling Native IP and Accessing a Device’s Native Features Using Virtual Network Addresses for Example 3

After creating the VPN tunnel as described in “IPSec VPN Configuration for Example 3” on page 362 or “PPTP VPN Configuration for Example 3” on page 364, the user enables native IP and accesses a device’s native features.

In this example, to access “sp4,” which is a type of service processor that does not work with virtual network addresses because it is not compatible with DNAT, the user would enter the OnBoard’s real address, as described in “Enabling Native IP and Accessing a Device’s Native Features Using Real IP Addresses for Example 2” on page 355.

Enabling Native IP Access for Example 3

In this example, to enable native IP access to "sp1," "sp2," or "sp3," the user would enter the OnBoard's virtual IP address, which is `172.20.0.1`, in one of the two following ways:

- In a browser on the user's workstation, the user would do the following:
  - Bring up the Web Manager using `http://172.20.0.1`.
  - Chose the Devices left menu option.
  - For either "sp1," "sp2," or "sp3," click "Enable Native IP access."
- On the user's workstation's command line, the user would do the following:
  - Use `ssh` to connect to the OnBoard's console and to access the `rmenush` menu in one of the following ways:

    `ssh` *`username`*`:@172.20.0.1`

    `ssh -t` *`username`*`:@172.20.0.` `menu`
  - Select "Access Devices" from the menu.
  - Select either "sp1," "sp2," or "sp3" from the devices menu.
  - Select "Enable native IP" from the list of management actions the user is authorized to perform on the device.

  OR

  - Use `ssh` to execute the `nativeipon` command directly using the device alias:

    `ssh` *`username`*`:`*`device_alias`*`@172.20.0.1` `nativeipon`

Accessing Native Features for Example 3

After enabling native IP access, the user can access one of the desired native features that may be available on the device, including:

- A native web application, which may be accessed in one of the following ways:
  - In the Web Manager on the OnBoard, clicking the "Go to native web interface" link on the Access Devices screen.
  - On the user's workstation, entering the virtual IP address of the device in a browser.

- On the user's workstation, on the command line, entering the `ssh` command with the name/alias of the device along with the virtual IP address of the OnBoard.

  For example, see the following `ssh` command line entered by the user named "allSPs" to access "sp2" using the OnBoard's virtual IP address `172.20.0.1`.

  ```
  ssh -t allSPs:sp2@172.20.0.1
  ```

- A management application, which may be accessed in one of the following ways, depending whether the application is a client on the user's workstation or resides on the service processor:
  - If the management application resides on the user's workstation, by bringing it up from there.
  - If the management application resides on the service processor, and is an executable that can be invoked on the command line, by accessing the service processor's console first in one of the following two ways:
    - Invoking `ssh` with the `spconsole` command in the following format

    ```
    ssh -t allSPs:sp2@172.20.0.1 spconsole
    ```

    OR

    - In the Web Manager on the OnBoard, clicking the "Service Processor Console" link on the Access Devices screen.

    AND

    - Bringing the management application up from the service processor's command line.
- The console of the server on which the service processor resides, in one of the following two ways:.
  - Invoking `ssh` with the `devconsole` command in the following format

    ```
    ssh -t allSPs:sp2@172.20.0.1 devconsole
    ```

    OR

  - In the Web Manager on the OnBoard, clicking the "Device Console" link on the Access Devices screen.

Options for Assigning IP Addresses to Connected Devices

After the addressing scheme is planned as described in "Understanding Address Configuration for Connected Devices" on page 336, the OnBoard administrator must do both of the following:

- Assign an IP address in the planned range of addresses when configuring each device on the OnBoard, as described in "Parameters for Configuring Devices" on page 58.
- Assign the same IP address on the device itself.

The available options for assigning IP addresses on the connected devices are summarized in the following bulleted list:

- A device may have a default IP address already assigned.

  In most cases, such a default IP address would not be used. Instead an IP address of the OnBoard administrator's choosing would probably be assigned from the site's private-side device IP addressing scheme, using one of the other available methods.

- The OnBoard administrator may directly configure a device with a static IP address.

  Configuration of a device's static IP address would be done using whatever means are available (such as a service processor's console port, the server's firmware setup, or software running on the server).

- If connected devices are running DHCP client software, then the OnBoard administrator can assign the desired fixed IP address to the device's MAC address in the `dhcp.conf` file, as described in "Configuring the DHCP Server" on page 26.

Additional Network Address Configuration Examples

Refer to PDF files about network address configuration in `/usr/share/docs/OnBoard/Application_Notes/Network`:

- `NativeIP.pdf`
- `VirtualIP.pdf`
- `priv-to-pub.pdf`

- `ssh_tunnel.pdf`
- `tftp.pdf`

B
Advanced Boot and Backup Configuration Information

This chapter provides information related to configuring boot file locations and managing configuration file changes.

Boot File Location Information	Page 372
Downloading a New Software Version	Page 375
Changing the Boot Image	Page 375
Network Boot Options and Caveats	Page 378
Options for the create_cf Command	Page 381
Options for the restoreconf Command	Page 384

This chapter also provides the troubleshooting procedures shown in the following sections.

To Boot from an Alternate Image Using cycli	Page 375
To Boot in U-Boot Monitor Mode	Page 377
To Boot from an Alternate Image in U-Boot Monitor Mode	Page 377
To Boot in Single User Mode from U-Boot Monitor Mode	Page 378
To Replace a Boot Image From a Network Boot in U-Boot Monitor Mode	Page 379
To Restore the OnBoard Configuration Files to the Last Saved Version	Page 380
To Restore the OnBoard Configuration Files to the Factory Defaults	Page 380

Boot File Location Information

How the OnBoard boots is introduced at a high level in “Configuring the Boot File Location” on page 152. The additional information in this section is to give an administrator who has the root password enough background to be able to boot from an alternate image if the need arises and if the Web Manager is not available.

The OnBoard uses a U-Boot boot loader that resides in soldered flash memory and that automatically runs at boot time. U-Boot boots the OnBoard from an image whose location is configurable. The image can reside either in a separate removable flash memory on the OnBoard or on a boot server on the network.

Up to two images may be stored at the same time on the OnBoard’s removable flash. Each image on the removable flash has three separate file systems mounted on three Linux partitions. The first partition for each image contains the kernel, the second partition contains the root filesystem mounted read only, and the third partition contains the configuration files mounted read-write.

For more about U-Boot in general, go to: http://sourceforge.net/projects/u-boot.

The OnBoard boots from alternate images as described below.

- The OnBoard initially boots from a software image referred to as “image1,” which is stored in three partitions on the removable flash (`hda1`, `hda5`, and `hda7`).
- The first time you download and install a new software version from Cyclades, the new image is stored as “image 2” in another set of three identical partitions on the removable flash (`hda2`, `hda6`, and `hda8`), and the configuration is changed to boot the OnBoard from “image2.”
- The second time you download a new software version, the latest image is stored as “image1” in the first set of three partitions, and the OnBoard configuration is changed to boot from “image1.”
- Subsequent downloads are stored following the same pattern, alternating “image1” with “image2.”

Refer to the following text and figure explaining partition numbers if needed for understanding some of the instructions in the rest of this chapter. As illustrated in the following figure, the first partition for each image contains the Linux kernel, the second partition contains the root-mounted filesystem (which is mounted read only), and the third partition (which is mounted read write) contains the configuration files.

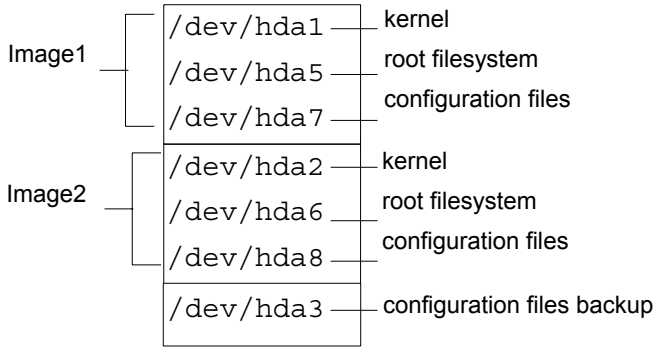


Figure B-1: Boot Partitions

The previous figure also shows a configuration backup partition (`/dev/hda3` in removable flash). This partition is mounted as `/mnt/hda3`. The `/mnt/hda3/backup` directory is used for storing compressed copies of backed-up configuration files, as shown in the following screen example.

```
[root@OnBoard root]# cd /mnt/hda3/backup
[root@OnBoard  backup]# ls
configuration_files.gz
```

Downloading a New Software Version

You can download a new software version in the following ways:

- Use the Web Manager Mgmt → Firmware Upgrade screen to download the image from an FTP server

  When the image is downloaded by FTP, a script (`saveimage`) automatically extracts the filesystem from the image, mounts it, and copies the files to the removable flash. Since the current image is being run from one of the three-partitions sets, the downloaded image is stored in the other set of three partitions. The environment variable `currentimage` is changed so that the system boots from the new image.

- Do a network boot from the image and then save it onto the removable flash

  The U-Boot monitor command `net_boot` boots the image from the TFTP server specified in the environment variables. After the image is downloaded by network boot, the root filesystem is in the RAMDISK, and the image can run even if no removable flash card is inserted.

  From the command line, you can then run the `create_cf` script with the `--doformat` option to automatically save the image from RAMDISK into the removable flash. The script erases everything in the flash, partitions the flash, if necessary, formats the partitions, and copies the files currently in the RAMDISK into the corresponding image partitions. If the flash is already partitioned, you can choose where the image is saved using the option `--imageN`.

Changing the Boot Image

If, for any reason, you want to change to another image from the current one, if you have access to the Web Manager, you can use the Config → Boot Configuration screen to select the other image, and then use the "Restart" button on the Mgmt → Restart screen to boot the OnBoard from the new location.

You have two other options if you cannot access the Web Manager:

- Use the `cycli` utility

  See "To Boot from an Alternate Image Using cycli" on page 375.
- Boot in U-Boot monitor mode and use the available boot commands

  See "To Boot in U-Boot Monitor Mode" on page 377.

▼ *To Boot from an Alternate Image Using cycli*

1. Connect to the OnBoard from a terminal connected to the console port or create a `telnet` or `ssh` connection, and log in as root.
2. Enter the `cycli` command.

   ```
   # cycli
   ```

   The `cli>` prompt appears.

   ```
   cli>
   ```

3. Enter the `get bootconf` command to check the current configuration to find out which boot command and boot image are being used.

   In the screen example, `hw_boot` is defined as the `bootcmd` and `image2` is defined as the image.

   ```
   cli> get bootconf
   ...
   bootconf bootcmd: hw_boot
   ...
   bootconf image: 2
   ```

4. To boot from a TFTP boot server over the network, do the following steps.

   a. Set the `bootcmd` to `net_boot`.

   ```
   cli> set bootconf bootcmd net_boot
   ```

   b. Specify the TFTP boot server's IP address.

   ```
   cli> set bootconf serverip IPaddress
   ```

   c. Specify the name of the boot file on the TFTP server.

   ```
   cli> set bootconf bootfile allImage.1129-qa0
   ```

   The `currentimage` environment variable is changed to boot from the specified image.

Changing the Boot Image in U-Boot Monitor Mode

You can access U-Boot monitor mode in one of the following two ways:

- During boot, when the "Hit any key to stop autoboot" prompt appears, pressing any key before the timer expires brings the OnBoard to U-Boot monitor mode.
- If boot fails, the OnBoard automatically enters U-Boot monitor mode.

The U-Boot `hw_boot` command boots from either the first or second image according to the value of the `currentimage` environment variable. You can use the following procedures to change which image is used for booting.

To Boot in U-Boot Monitor Mode	Page 377
To Boot from an Alternate Image in U-Boot Monitor Mode	Page 377
To Boot from an Alternate Image Using cycli	Page 375
Changing the Boot Image in U-Boot Monitor Mode	Page 376
To Boot in Single User Mode from U-Boot Monitor Mode	Page 378

▼ To Boot in U-Boot Monitor Mode

1. Open a terminal connection to the console port, and log in as root.
2. Enter the `reboot` command.

```
# reboot
```

3. During boot, when the “Hit any key to stop autoboot” prompt appears, press any key before the time elapses to stop the boot.

   The U-Boot monitor prompt appears:

```
=>
```

4. Enter `help` to see a list of supported commands.

```
=> help
```

▼ To Boot from an Alternate Image in U-Boot Monitor Mode

1. Go to U-Boot monitor mode.

   See "To Boot in U-Boot Monitor Mode" if needed.

2. Set the current image environment variable to the number of the image you want to boot.

```
=> setenv currentimage N
```

   For example, to boot from image2 enter the number 2, as shown in the following screen example.

```
=> setenv currentimage 2
```

3. Enter the boot command.

```
=> hw_boot
```

▼ *To Boot in Single User Mode from U-Boot Monitor Mode*

1. See "To Boot in U-Boot Monitor Mode" on page 377 if needed.
2. Boot by entering `hw_boot` followed by `single`, as shown in the following screen example.

```
=> hw_boot single
```

3. The single-user # prompt appears, as shown in the following screen example.

```
[root@(none) /]#
```

Network Boot Options and Caveats

When a network boot is performed with the U-boot `net_boot` command, the OnBoard boots from the specified image on the TFTP server. The image uses the RAMDISK as the root file system. Network boots are useful for troubleshooting because the net-booted image can run even if there the OnBoard's flash memory is not usable.

Network boots are recommended only for troubleshooting and must not be used for normal operation of the OnBoard. For example, if you want to test a new release of the software to make sure a problem is fixed, or if the removable flash memory becomes corrupted, you could download the software to a tftpboot server, and then save it to the removable flash after testing, using the `create_cf` command with the appropriate options (see "Options for the create_cf Command" on page 381).

When a network boot is performed, the system uses one of the two following sources of configuration data:

- If the `net_boot` command is entered with the `configsource=factory_default` option, the factory_default configuration files are restored.
- Otherwise, the backed up configuration files from the `/dev/hda3` backup partition are copied to the RAMDISK and used.

Any configuration changes made after the last backup copy was made are lost unless the configuration files were backed up before the network boot and

then restored afterwards (see “Backing Up Configuration File Changes” on page 68 and “Restoring Backed Up Configuration Files” on page 69).

▼ *To Replace a Boot Image From a Network Boot in U-Boot Monitor Mode*

1. Log in as root in U-boot monitor mode.

   If needed, see, “““To Boot in U-Boot Monitor Mode” on page 377.

2. Set the “bootfile,” “serverip,” and “ipaddr” environment variables using the boot filename, the TFTP boot server’s IP address, and the IP address of the OnBoard to use for network booting.

   The format of the boot filename is: `zmppcons.v`*`version_number`*, for example: `zmppcons.v120`.

```
=> setenv ipaddr OnBoard's_IP_address
=> setenv serverip boot_server's_IP_address
=> setenv bootfile boot_file's_name
```

   See the following screen example.

```
=>setenv ipaddr 193.168.45.29
=> setenv serverip 193.168.46.127
=> setenv bootfile zvmppconb.v101
```

3. Check that the environment variables are set properly with the `printenv` command.

```
=> printenv
bootfile=zvmppconb.v120
ipaddr=192.168.48.113
serverip=192.168.49.127
```

4. Enter the `net_boot` command.

```
=> net_boot
```

5. Log in as root after boot completes.
6. Run the `create_cf` command with the `--doformat` option.

```
[root@OnBoard root]# create_cf --doformat --factory_default
```

Note: Be aware that the `--doformat` option erases the flash memory and installs the boot image into the image1 area. See "Options for the create_cf Command" on page 381 for other options.

7. The following text appears when the operation completes.

```
Creation of image N completed.
...
```

8. Configure the OnBoard to boot from flash.

   See "To Boot from an Alternate Image in U-Boot Monitor Mode" on page 377, if needed.

9. Enter the `reboot` command.

```
# reboot
```

▼ *To Restore the OnBoard Configuration Files to the Last Saved Version*

This procedure assumes that you or a previous administrator has previously run the `saveconf` command, or clicked the "Save" button on the Web Manager Mgmt → Backup/restore screen after making changes to the configuration. This procedure restores the configuration files to the state they were in when they were last backed up.

1. If you are logged into the Web Manager as an administrative user, click the "Load" button on the Web Manager Mgmt → Backup/restore screen.

2. If you are logged into the OnBoard console as root through the console port, via `telnet` or `ssh`, enter the `restoreconf` command.

```
[root@OnBoard root]# restoreconf
```

▼ *To Restore the OnBoard Configuration Files to the Factory Defaults*

Use one of the commands shown below while logged in as root through the console, via `telnet`, or via any `ssh` session to restore the configuration files to the state they were in when the OnBoard shipped.

- Enter the `restoreconf` command with the `factory_default` option.

```
[root@OnBoard root]# restoreconf factory_default
```

- Enter the `create_cf` command with the `--factory_default option.`

```
[root@OnBoard root]# create_cf --factory_default
```

Options for the create_cf Command

You can use the `create_cf` command when troubleshooting problems with the boot image, as described under “To Replace a Boot Image From a Network Boot in U-Boot Monitor Mode” on page 379. Use it carefully as described in this section.

Only use the `--doformat` option to save the image that is currently in RAM into the image1 area, but be aware that this option reformats all flash partitions while saving the image.

Use the `--image[1|2]` option to save the image that is currently in RAM into a specific image area, without reformatting the partitions that contain the other image.

The following table provides more information about the `create_cf` command options, which you can view from the Linux command line by entering the name of the command.

Table B-1: Options for the create_cf command

Option	Description
none	Not recommended. Checks if a boot image is already on the device. If no image is on the device (as would be true for a newly installed removable flash on a PCMCIA card) and if no image is specified, runs `--doformat` and installs the image in image1. If multiple images are on the device, and no image is specified, presents a choice of images for the user to choose from, and then writes the image from RAM into the specified image area. In either case, restores the factory default configuration
`-d` *`device`*	Creates the image on the specified device. The default device is `/dev/hda` (the removable flash memory). Make sure the filesystem is not mounted. Use the `-d` device option if you want to create the image in another location, such as an installed compact flash PCMCIA card. (The device names for PCMCIA cards are determined by the number of the card slot where the card is installed, either `/dev/hdc` (PCMCIA slot 1) or `/dev/hde` (PCMCIA slot 2).
`--factory_default`	Creates the image with factory default configuration values. By default, if this option is not entered, the configuration from the current partition is used, if valid.
`--doformat`	Rebuilds the partitions, erasing their contents. Creates the image as image1.
`--dontformat`	Does not format the compact flash. The sizes of partitions hda1-3 and 5-8 are checked. If the partition sizes are not smaller than 2, 2, 5, 51, 51, 6, and 6 Mbytes respectively, the image is installed in the specified image area.

Table B-1: Options for the create_cf command (Continued)

Option	Description
`--image`*N*	Creates/replaces image*N*, when n=1 | 2. Use this option to replace only the specified image without erasing both images. Changes the `currentimage` environment variable to boot from the image.

Examples for create_cf Command Usage

All the examples assume you have done a network boot and you want to save the image from RAM.

Saving an Image to a Flash PCMCIA Card

After inserting a flash memory PCMCIA card into PCMCIA slot 1, you would enter the following command to save a copy of the image from RAM into the flash memory PCMCIA card in PCMCIA slot 1.

```
[root@OnBoard /]# create_cf --/dev/hdc --image1
```

Saving an Image into the Image2 area and Restoring the Factory Default Configuration.

The following command saves the image from RAM into the image2 area and restores the factory default configuration.

```
[root@OnBoard /]# create_cf --factory_default --image2
```

Options for the restoreconf Command

As described in other sections of this chapter, you may need to use the `restoreconf` command while troubleshooting. All the `restoreconf` subcommands are shown in the following screen example.

```
restoreconf:

Usage:

Restore from flash:           restoreconf

Restore from factory default: restoreconf factory_default

Restore from storage device:  restoreconf sd

Restore from local file:      restoreconf local <FILE>

Restore from FTP server:      restoreconf ftp <FILE>
<FTP_SERVER> <USER> <PASSWORD>

Restore from TFTP server:     restoreconf tftp <FILE>
<TFTP_SERVER>

Restore from SSH server:      restoreconf ssh <FILE>
<SSH_SERVER> <USER>
```

Glossary

1U

One rack unit (also referred to as 1RU). A standard measurement equal to 1.75” (4.45 cm) of vertical space on a rack or cabinet that is used for mounting computer equipment.

3DES

Triple Data Encryption Standard, an encrypting algorithm (cipher) that encrypts data three times, using a unique key each time, to prevent unauthorized viewers from viewing or changing the data. 3DES encryption is one of the *security features* provided by Cyclades products to enable customers to enforce their data center security policies. See also *authentication*, *authorization*, and *encryption*.

ActiveX

A set of technologies developed by Microsoft from its previous OLE (object linking and embedding) and COM (component object model) technologies. Browsers used for accessing KVM output from devices connected to Cyclades AlterPath KVM products must have ActiveX enabled.

advanced lights out manager (See *ALOM*)

AH (*authentication header)*

One of the two main protocols used by IPSec. (*ESP* is the other). AH authenticates data flowing over the connection. AH is not compatible with *NAT*, so it must be employed only when the source and destination networks can be reached without NAT. Does not define the authentication method that must be used.

alias

An easy-to-remember, usually-short, usually-descriptive name used instead of a full name or IP address. For example, on some Cyclades products, port names contain numbers by default (as in Port_1) but the administrator can assign an alias (such as *SunBladeFremont* that describes which server is connected to the ports. Aliases make it easier for users to understand which devices are connected.

ALOM (advanced lights out manager)

A service processor on certain Sun servers that includes an independent system controller and firmware. Provides remote monitoring, logging, alerting, and basic control of the server.

application-specific integrated circuit (See *ASIC*)

ASIC (Application-Specific Integrated Circuit)

Pronounced “ay-sik”. A type of chip used for applications that provide a specific function, such as an ASIC chip that serves as a *BMC*.

authentication

The process by which a user’s identity is checked (usually by checking a user-supplied username and password) before the user is allowed to access requested resources. Authentication may be done locally (on the Cyclades device) or on a configured authentication server running one of the widely-used authentication protocols (LDAP, RADIUS, TACACS+, NIS, SMB, and Kerberos) that are supported by Cyclades products. Authentication is one of the *security features* provided on Cyclades products to enable customers to enforce their data center security policies. See also *authorization* and *encryption*.

authentication header (See *AH)*

authorization

Permission to access a controlled resource, which must be granted by administrative action. A user’s authorizations are checked after a user logs into a system and has been authenticated. Each user is restricted to using only the features the user is authorized to access. Checking a user’s authorizations

is one of the *security features* provided on Cyclades products to enable customers to enforce their data center security policies. A user who is authorized to access a device or software function is referred to as an *authorized user*. See also *authentication* and *encryption*.

authorized user

One who is given permission to access a controlled resource, which must be granted by administrative action.

backup configuration

On Cyclades products, specifies where to save compressed configuration files for possible later restoration. Some Cyclades products save configuration changes in the affected configuration files while maintaining a backed-up compressed set of configuration files in a separate directory. The backup directory's contents are available for restoration until the administrator takes a specific action to overwrite the backed-up files.

baseboard

A gender-neutral term for "motherboard."

baseboard management controller (See *BMC*)

basic input/output system (See *BIOS*)

baud rate

Pronounced "bawd rate." When configuring terminal or modem settings on serial ports and console port connections on AlterPath devices, the specified baud rate must match the baud rate of the connected devices.

Options range from 2400–921600 bps. 9600 is the most-common baud rate for devices.

BIOS (basic input/output system

Pronounced “bye-ose.” Instructions in the onboard flash memory that start up (boot) a computer without the need to access programs from a disk. Sometimes used for the name of the memory chip where the start-up instructions reside. BIOS access is available even during disk failures. Administrators often need to access the BIOS while troubleshooting, for example, to temporarily change the location from which the system boots in case of a corrupted operating system kernel. How to access the BIOS varies from one manufacturer to the other.

BMC (baseboard management controller)

An internal processor on some servers that is separate from the main system and that operates even if the main processor is not operable. Sits on the server’s baseboard (motherboard), on an internal circuit board, or on the chassis of a blade server. Monitors on-board instrumentation. Provides remote reset or power-cycle capabilities. Enables remote access to BIOS configuration or operating system console information. In some cases provides *KVM* control of the server. Includes a communication protocol that delivers the information and control to administrators.

bonding

See *Ethernet bonding*.

callback

A *security feature* used to authenticate users who are calling into a device. The software authenticates the user, hangs up, and then returns the call to the user before allowing access.

CAT5 (category 5)

A standard for twisted-pair Ethernet cables defined by the Electronic Industries Association and Telecommunications Industry Association (commonly known as EIA/TIA).The support for CAT5 and later cabling (such as CAT5e) in many Cyclades products allows the use of existing cabling in the data center.

CDMA (code division multiple access)

A mobile data service available to users of CDMA mobile phones.

CHAP (challenge handshake authentication protocol)

An authentication protocol used for PPP authentication. See MS-CHAP.

checksum

Software posted at the Cyclades download site is accompanied by a checksum (`*.md5`) file generated using the MD5 algorithm. The checksum of a downloaded file must be the same as the checksum in the file. The checksum is compared automatically when the download is performed through the Web Manager or can be compared manually if the download is performed using `ftp` or `http`. If the checksums do not match, the software file is damaged and should not be used.

CLI (command line interface)

Allows users to use text commands to tell computers to perform actions (in contrast to using a GUI). The user types a text command at an on-screen prompt and presses the Enter or Return key. The computer processes the command, displays output when appropriate, and displays another prompt. Users can save a series of frequently-used commands in a script. Being able to create and run scripts to automate repetitive tasks is one of the reasons many administrators prefer using a CLI.

Cyclades products run the Linux operating system, and most Cyclades products allow access to the command line of the Linux shell. Command line access is achieved through several different means. For one example, a remote administrator can use Telnet or SSH to access an AlterPath OnBoard and then can enter commands on the Linux shell's command line.

Some Cyclades products offer a management utility called the CLI. Administrators type “CLI” or “cli” at the prompt in the Linux shell. Products that provide similar utilities with different names, such as the AlterPath OnBoard `cycli`, provide an alias for users who are familiar with the CLI name. The Cyclades CLI tool provides many commands and nested parameters in a format called the *CLI parameter tree*.

CLI parameter tree

Each version of the Cyclades *CLI* utility has a set of commands and parameters nested in the form of a tree. The CLI for the AlterPath OnBoard and other products use the Cyclades Application Configuration Protocol (CACP) daemon (cacpd). The cacpd uses the `param.conf` file, which defines a different CLI parameter tree for each product.

client-side management software—See *management software*

command line interface (See *CLI*)

community name

A string used as a type of shared password by *SNMP* v1 and v2 to authenticate messages. Hosts that share the same community name usually are physically near each other. The administrator must supply a community name when configuring SNMP on the Cyclades device, and the same community name must be also configured on the SNMP server. For security reasons, the default community name *public* cannot be used.

console

A computer mode that gives access to a computer's command line (see *command line interface*). The console also displays error messages generated by the computer's operating system or *BIOS*. Console access is essential when a device (such as some special-purpose servers, routers, service processors, and other embedded devices) has no window system. Console access is also essential when the window system is not available on a device that has one, either because the system is damaged or it is offline. Access to the console allows remote administrators to control and repair damaged or otherwise-unavailable systems. See also *device console* and *service processor* console.

console servers

Appliances that give consolidated access to the console ports of connected assets, either over the network, through dial-in, or direct serial connection.

Cyclades

A corporation founded in 1989 to provide unique networking solutions. Named after the ground-breaking French packet-switching network created in 1970, which was named after the Greek province of Cyclades. Cyclades in Greece is made up of many islands that when viewed on a map resemble a diagram of nodes in a computer network.

decryption

Decoding of data that has been encrypted using an *encryption* method.

Dell Remote Assistant Cards (See *DRAC*)

Dell Remote Administrator Controller (See *DRAC*)

device console

The console on a server or another type of device that allows access to its console through an Ethernet port that is connected to one of the OnBoard's private Ethernet ports.

DHCP (dynamic host configuration protocol)

A service that can automatically assign an IP address to a device on a network, which saves administrator's time and reduces the number of IP addresses needed. Other configuration parameters may also be managed. A DHCP server assigns a dynamic address to a device based on the *MAC address* of the device's Ethernet card. Many Cyclades devices are shipped with DHCP client software, and with DHCP enabled by default.

dial-in

A method of connecting to a remote computer using communications software, such as *PPP*, along with a modem, and a telephone line, which is supported on many Cyclades products. After the administrator of the Cyclades product has connected a modem from the Cyclades product to a live telephone line and made the phone number available, a remote authorized user can use the phone number to dial into the Cyclades product and access connected devices.

DNS (domain name service or system)

A service that translates domain names (such as `cyclades.com`) to network IP addresses (192.168.00.0) and that translates host names (such as "onboard") to host IP addresses (192.168.44.11). To enable the use of this service, administrators need to configure one or more DNS servers when configuring AlterPath devices.

DRAC (Dell Remote Access Controller)

All of the following combinations are used for defining this acronym, with multiple definitions appearing even at the Dell website: Dell Remote [Access | Administrator | Administration] [Controller | Card].

Service processors on certain Dell servers may include an independent DRAC system controller. Several incompatible version types exist (DRAC II, DRAC III, DRAC III/XT, DRAC IV) along with several incompatible firmware versions. All controller types have a battery and can have an optional PCMCIA modem installed. Provide remote monitoring, logging, alerting, diagnostics, and basic control of the server. Some types have a *native web interface* and a *native application* "Dell OpenManage Server Administrator," that runs on the remote administrator's computer. Dell Open ManageIT Assistant software on the administrators computer can be used to configure and launch access.

The OnBoard provides access to many but not all DRAC management functions on supported DRAC versions. To access all the management functions available through DRAC requires *native IP* access.

encapsulating security payload (See *ESP*)

encryption

Translation of data into a secret format using a series of mathematical functions so that only the recipient can decode it. Designed to protect unauthorized viewing or modification of data, even when the encrypted data is travelling over unsecure media (such as the Internet). See 3DES and SSH. As an example, a remote terminal session using secure shell SSH usually encrypts data using 3DES or better algorithms. Encryption is one of the security features provided on Cyclades products to enable customers to enforce their data center security policies. See also *authentication* and *authorization*.

ESP (encapsulating security payload)

One of the two main protocols used by IPSec (*AH* is the other). ESP encrypts and authenticates data flowing over the connection. Does not define the authentication method that must be used. DES, 3DES, AES, and Blowfish are commonly used with ESP.

Ethernet bonding

Synonymous with *Ethernet failover*. A way of configuring two Ethernet ports on a single device with the same IP address so that if the primary Ethernet port becomes unavailable, the secondary Ethernet port is used. When bonding is enabled, the active IP address is assigned to bond0 instead of eth0. When the primary Ethernet port returns to active status, the software returns it to operation.

Ethernet failover

See *Ethernet bonding*. See also *failover*.

event log

Referred to as the system event log (SEL) on most service processors, a timestamped record of events such as power on/off, device inserts/removals/ connects/disconnects, sensor threshold events and alerts.

Expect script

A script written using `expect`, a scripting language based on Tcl, the Tool Command Language. Can be written to perform automation and testing operations that are not possible with other scripting languages. Cyclades uses `expect` scripts in some of its AlterPath products, and users can customize some of the default expect scripts. For example administrators of the AlterPath OnBoard can customize the Expect scripts that handle conversations with service processors and other supported devices.

failover

A high-availability feature that relies on two redundant components in a system or a network, with the second component available to automatically take over the work of the primary components if the primary component becomes unavailable for any reason. When the primary component becomes available, it takes over the work again. Automatically and transparently redirects requests from the unavailable component to the backup component. Used to make systems more fault-tolerant. See *Ethernet bonding*.

flash memory

A chip used to store the operating system, configuration files, and applications on some Cyclades products.

GPRS (general packet radio service)

A mobile data service available to users of GSM mobile phones that adds packet data capabilities.

GSM (global system for mobile communications)

Originated by the GSM (Groupe Special Mobile) group in France in 1982. A popular standard for mobile phones.

GUI

Graphical user interface (pronounced GOO-ee). A computer interface that allows users to tell computers to perform actions by clicking on graphical elements such as icons, choosing options from menus, and typing in text fields on forms displayed on the computer screen. Many Cyclades products provide GUI access through the Cyclades Web Manager.

HTTP (hypertext transfer protocol)

Protocol defining the rules for communication between Web servers and browser across the Internet.

HTTPS (secure HTTP over SSL)

Protocol enabling the secure transmission of Web pages by encrypting data using *SSL* encryption. URLs that require an SSL connection start with `https`.

IETF (Internet Engineering Task Force)

Main standards organization for the Internet. Working groups create Internet Drafts that may become RFCs. RFCs that are approved by the Internet Engineering Steering Group (IESG) may become standards. RFCs (Requests for Comments) are the official technical specifications of the Internet protocol suite. For example, the format of *SNMP MIBs* was defined by the IETF, which assigns MIB numbers to organizations.

iLO (Integrated Lights Out)

Hewlett Packard's proprietary service processor (pronounced *EYE-loh*). Even though HP is a major supporter of IPMI, the company also provides iLO because it provides many more functions than IPMI. The iLO processor resides on the *baseboard*. Even if the server is off, iLO is active. When the dedicated Ethernet port is plugged into the network, iLO uses DHCP. iLO has a web interface and a Telnet interface. Advanced iLO provides remote KVM and *virtual media* access.

integrated lights out (See *ILO*)

IP address consolidation

Provides controlled access to basic management features on multiple Ethernet-based servers that have embedded service processors, using only one Internet address. When managed separately, each service processor needs its own IP address. Managing multiple servers with multiple IP addresses is both expensive and time consuming without consolidation.

IPDU (intelligent power distribution unit)

A device with multiple power inlets into which IIT assets can be plugged for remote power management. Cyclades supports a family of AlterPath PM IPDUs that can be remotely managed when they are connected to AlterPath devices, such as the AlterPath KVM/net or AlterPath OnBoard.

IPMI (Intelligent Platform Management Interface)

An open standards vendor-independent service processor currently adopted by many major server platform vendors. Its main benefit over other service processor types is that it is installed on servers from many vendors, providing one interface and protocol for all servers. Its main disadvantage is that it does not always provide as much functionality as the proprietary service processors. For this reason, IBM's series e325 and e326 servers use IPMI to manage their BMCs but the top-of-the-line xSeries servers use *RSA II*. IPMI works by interacting with the *BMC*, and since it usually has standby power, it can function even if the operating system is unavailable or if the system is powered down. The OnBoard supports IPMI version 1.5. OnBoard administrators can create custom *Expect* scripts to support IPMI 2.0.

ipmitool

A command line utility that interfaces with any *BMC* that supports either IPMI 1.5 or 2.0 specifications. Reads the sensor data repository (SDR) and prints sensor values, displays the contents of the System Event Log (SEL), prints Field Replaceable Unit (FRU) inventory information, reads and sets LAN configuration parameters, and performs remote chassis power control. Described at SourceForge at: `http://ipmitool.sourceforge.net`. The command options are described on the `ipmitool`(1) man page at SourceForge: `http://ipmitool.sourceforge.net/manpage.html`. `ipmitool` commands can be added to customized scripts on the OnBoard to access unsupported features on a connected service processor.

IPSec (Internet protocol security)

A suite of protocols used for establishing private, secure, connections over IP networks. Only the sending and receiving computers need to be running IPSec. Each computer handles security at its end and assumes that the intermediary nodes between the source and destination computers are not

secure. Supported on many AlterPath products. In tunnel mode, IPSec is used to form a *VPN* connection, creating a secure tunnel between either an individual host or a subnet on one end and the AlterPath device on the other end. Has two modes, *transport* and *tunnel* mode. Tunnel mode encrypts the entire packet. Transport mode encrypts application headers, TCP or UDP headers, and packet data, but not the IP header. The method that encrypts the entire packet cannot be used where NAT is required

Kerberos

Network *authentication* protocol designed to provide strong authentication for client/server applications by using secret-key cryptography.

KVM

Remote keyboard, video [monitor], and mouse access to a server through a PS/2 or USB connection on a server that is connected to a KVM switch.

KVM analog switch

A *KVM switch* that requires a local user connection before a user can gain access to any servers that are connected to the switch. Cyclades AlterPath KVM analog switches are one component of the *out-of-band infrastructure*.

KVM over IP switch

A *KVM switch* that supports remote access over a LAN or WAN or telephone line to servers connected to the switch, using the TCP/IP protocols and a web browser. Enables operations over long distances. Cyclades AlterPath KVM/IP switches are one component of the *out-of-band infrastructure*.

KVM switch

Enables use of only one keyboard, video monitor, and mouse to run multiple servers from a remote location. Reduces expenses by eliminating the cost of acquiring, powering, cabling, cooling, managing, and finding data-center space for one keyboard, monitor, and mouse for every server. Servers are connected to KVM ports on Cyclades AlterPath KVM switches using AlterPath KVM terminators on the server end and up to 500 feet of *CAT5* or greater cable. AlterPath KVM switches provide *authentication* and other *security features* and allow only *authorized users* to access a restricted set of connected servers. See also *KVM analog switch* and *KVM over IP switch*.

Cyclades AlterPath KVM analog switches are one component of the *out-of-band infrastructure*.

LDAP (lightweight directory access protocol)

A directory service protocol used for authentication. One of many standard authentication protocols supported on Cyclades devices.

MAC address

Also called the Ethernet address. A number that uniquely identifies a computer that has an Ethernet interface. Cyclades equipment displays MAC addresses on a label on the bottom.

management console—See service processor

management network

A network separated from the *production network* that provides remote *out-of-band* access for management of IT assets, including access for returning disconnected IT assets to service without the need for a site visit.

management software

Each server company that offers a service processor produces its own client-side software to access the servers' management features through the service processor. In some cases, management software is imbedded in the service processor and is presented either as a web interface or as a command line interface accessed using SSH or Telnet, or as both a web interface and command line interface. In other cases, the management software is installed in a client workstation and accesses the management features of the service processor using an IP-based protocol, such as *IPMI*. Most of these types of software only manage one server, do not scale, and do not address the need for consolidated access-control, multi-user access, data logging, and event detection, encyrption and other needs. The OnBoard addresses these needs and provides a single interface to access basic features of multiple-vendors' service processors.

MIB

Each *SNMP* device has one or more MIBs (management information bases), which describes the device's manageable objects and attributes. The MIB name tree for Cyclades starts at 1.3.6.1.4.1.4413.

MIIMON

A value set when configuring Ethernet failure to specify how often the active interface is inspected for link failures. A value of zero (0) disables MII link monitoring. A value of 100 is a good starting point, according to SourceForce bonding documentation.

MS-CHAP (Microsoft challenge handshake authentication protocol)

The Microsoft version of CHAP, which does not require the storage of a clear or reversibly-encrypted password. Can be used with or without AAA (authentication, authorization, and accounting). If AAA is enabled, PPP authentication can be done by TACACS+ and RADIUS.

NAT

Network address translation, an Internet standard that enables the use of one set of IP addresses for internal traffic and another set of IP addresses for traffic over the public network. The AlterPath OnBoard uses NAT to allow access to service processors and managed devices while not revealing their Ethernet addresses. Users can use administratively-assigned virtual IP addresses to access the service processor or device through the OnBoard.

native applications

A management option that gives the user the ability to run *service processor*-specific *native applications* and access the application's management features from the user's remote computer through the OnBoard. For example, the IBM service processor provides the IBM Director native application.

To obtain this type of access, the authenticated and authorized user selects the "Native IP" option after establishing a VPN connection between the user's computer and the OnBoard. At that point, the user can bring up the management application from where it resides on the user's computer or on the service processor and use the service processor's server management functions.

n*ative command interface* (See *NCI*)

native IP

A management option that the OnBoard administrator can enable when configuring a *service processor*. Because this option provides full access to all features supported by the service processor, the user must be a trusted user who is specifically authorized to use the option. A *VPN* connection must be made before the user is allow to access the native IP option. When the OnBoard user activates Native IP for a service processor, the OnBoard routes packets between that user's IP address and the service processor through a secure tunnel. The VPN connection must remain active for the duration of the Native IP session. Authorizing a user for native IP gives the user access to a *native application* or a *native web interface* that may be provided by the service processor and that may provide additional management functions beyond those provided by the OnBoard, including *KVM over IP* access to the server.

native web interface

A service processor feature that allows browser access to the service processor's information, management, configuration, and actions, by means of a HTTP/HTTPS server running on the service processor. Access to this feature requires the user to be authorized for *native IP*.

NCI (native command interface)

A *service processor* feature that allows direct access to the *console* of the service processor. Access may be provided to features such as power control, hardware auditing, event logs, sensor readings, and service processor configuration, usually by means of a Telnet or *SSH* server running on the service processor.

NEBS (Network Equipment Building System) Certification

Means that equipment has been tested and proven to meet the NEBS requirements for central office equipment that is adhered to in common by several telecommunications carriers. The requirements are in place to ensure that telecommunications equipment poses no risk or safety hazard to people, nearby equipment, or to the physical location where the equipment operates, and that equipment is reliable and dependable during both normal and abnormal conditions. Tests address heat release, surface temperature, fire

resistance, electromagnetic capability, electrical safety, and manufacturing component characteristics, among other attributes.

network time protocol (See *NTP*)

netmask

The dotted-decimal expression that determines which portion of an IP address represents the network IP address and which is used for host IP addresses, for example, 255.0.0.0.

NIS (Network Information Service)

A directory service protocol used for authentication in UNIX systems. One of many standard authentication protocols supported on Cyclades devices.

NTLM (NT LAN manager)

An authentication protocol used by Microsoft *SMB*.

NTP (network time protocol)

A protocol used to synchronize the time in a client with a high-accuracy network time protocol server.

OID

A unique indentifier for each object in an *SNMP MIB*. The OID naming scheme is in the form of an inverted tree with branches pointing downward. The OID naming scheme is governed by the IETF, which grants authority for parts of the OID name space to individual organizations. Cyclades has the authority to assign OIDs that can be derived by branching downward from the node in the MIB name tree that starts at 1.3.6.1.4.1.4413.

SNMP programs use the OID to identify the objects on each device that can be managed by using SNMP.

onbdshell

The OnBoard shell, `/usr/bin/onbdshell`, which displays a menu of devices an authorized user can access. Accessed by authorized users through selecting the “Access Devices” option from the user shell menu, *`rmenush`*. Selecting a server name from the menu brings up the list of actions the user is

authorized to perform on that server's *service processor*. Accessed by administrators by typing `/usr/bin/onbdshell` on the OnBoard's command line; the administrators' version of the menu lists all configured devices.

OOBI (Out-of-band Infrastructure)

An integrated systems approach to remote administration. Consists of components that provide secure, *out of band* access to connect to and manage an organization's *production network*. Components can include console servers, KVM and *KVM over IP* switches, power control appliances, centralized management devices (to control the entire out-of-band infrastructure), and service-processor managers to manage access to multiple vendor's service processors. Allows administrators to remotely connect to disconnected IT assets and to quickly return them to normal operation. Cyclades AlterPath products are designed as building blocks for an OOBI, including AlterPath ACS console servers, AlterPath KVM and KVM over P switches, AlterPath OnSite with consolidated console and KVM ports, AlterPath PM IPDUs, the AlterPath OnBoard service- processor manager, and the AlterPath Manager for centralized control of and access through multiple AlterPath devices to up to 5000 connected devices, and for access to servers that have IPMI controllers.

OTP (one-time passwords)

An authentication system that requires the user to generate and use a new password for every connection. The OTP can only be used once, which ensures that a discovered password is useless. Originally developed at Bellcore (now Telcordia), it started as a freely available program called S/Key that was trademarked. A newer freeware OTP program is OPIE (one time passwords in everything).

out of band

Access to IT assets that is either separate from or independent of the normal *production network*. A term that originated in the telecommunications industry to refer to communications used to control a phone call that are made on a dedicated channel, which is separate from the channel over which the call is made. Allows remote monitoring and control even when a managed IT asset loses connection to the production network. Typically, out-of-band access is through a *console* or management port (typically an RS-232 or Ethernet port),

an *intelligent power management device* (IPDU), a *KVM* port, or a *service processor.*

point to point protocol (See *PPP*)

point to point tunneling protocol (See *PPTP*)

PPP (point to point protocol)

A method that creates a connection between a remote computer and a Cyclades device and enables a remote user access using the Web Manager or the command line. Supports the use of the PAP, SPAP, CHAP, MS-CHAP, and EAP authentication methods.

PPTP (point to point tunneling protocol)

A *VPN* method developed by Microsoft along with other technology companies, it is the most widely supported VPN method among Windows clients and the only VPN protocol built into Windows 9x and NT operating systems. Uses the same types of authentication as PPP.

production network

The network on which the primary computing work of an organization is done. Users on a production network expect 24/7/365 availability with access to data and resources as reliable as access to telephone service. Development and testing of new applications are often performed on separate networks to avoid burdening or compromising the production network. Organizations often set up separate *management networks* to provide remote *out-of-band* access to disconnected IT assets.

RADIUS (remote authentication dial in user service)

A widely-supported authentication protocol for centralized user administration. Used by many Internet Service Providers (ISPs) and by devices such as routers and switches that do not have much storage. Combines authentication and authorization in a user profile. Relies on the UDP protocol. One of many standard authentication protocols supported on Cyclades devices.

remote supervisor adapter II (See *RSA II*)

remote system control (See *RSC*)

rmenush

The default login shell for users (`/usr/bin/rmenush`), which allows users only a limited set of menu options, including: access to management actions on devices for which they are authorized; the ability to change the user's password; and the ability to logout. The OnBoard administrator may modify the menu options and commands.

RSA II (remote supervisor adapter II)

Service processor technology on certain IBM servers that includes a service processor PCI card used to manage the BMC that is located on the motherboard. Enables the remote administrator to receive notifications, alerts, to view event logs and the last screen before a failure, to use virtual media (also called "remote media"), to control power and to manage the console through a web browser using a built-in Web server. Provides more options than the IPMI service processor that is available on IBM xseries e325 and e326 servers.

RSC (remote system control)

Service processor technology on certain Sun servers that includes a *service processor* RSC card. Enables the remote administrator to run diagnostic tests, view diagnostic and error messages, reboot the server, and display environmental status information from a remote console even if the server's operating system goes offline. The RSC firmware runs independently of the host server, and uses standby power drawn from the server. The RSC card on some servers include a battery that provides approximately 30 minutes of power to RSC in case of a power failure.

secure rack management (See *SRM*)

security features

Cyclades products provide security features, including *encryption*, *authentication*, and *authorization*, to enable customers to enforce their data

center security policies while providing *out-of-band* access to managed systems.

SEL (See *event log*)

serial over LAN (See SoL)

service processor (See SP)

service processor console

The console on a service processor whose dedicated Ethernet port is connected to one of the OnBoard's private Ethernet ports. Sometimes referred to as NCI (for native command interface). [OnBoard only]

service processor manager

An *OOBI* component that provides to users and groups secure, controlled access to basic features required for out-of-band management of servers that have embedded management controllers (also called *BMC*s or *service processors*). Also provides access to the console of servers and other devices without service processors but that have Ethernet ports that allow console access. Provides a single point of access through a single Ethernet address (see *IP address consolidation*) to services that are provided by service processors from several different vendors and to the console of certain servers and other devices. Its administrators are able to use a single interface to manage multiple servers without having to learn multiple management interfaces. The AlterPath OnBoard is the Cyclades service processor manager.

shell

A command interpreter on UNIX-based operating systems (like the Linux operating system that controls most Cyclades products). A shell typically is accessed in a terminal window where the shell presents a prompt. For example: `[admin@OnSite admin]#` is the prompt that appears when a user logs into an OnSite as admin and is in the `/home/admin` directory. Users tell the operating system to perform actions by typing commands in the shell, which interprets the commands and performs the specified actions. See also *command line interface*. The AlterPath OnBoard has two user shells: `onbdshell` and `rmenush`.

simple mail transfer protocol (See *SMTP*)

SMB (server message block)

A protocol used for file sharing and other communications between Windows computers. Microsoft uses this protocol along with NTML authentication protocol used to authenticate a client on a server.

SMTP (simple mail transfer protocol)

The most-commonly-used protocol used to send email.

SNMP (simple network management protocol)

A set of network management protocols for TCP/IP and IPX (Internet Packet Exchange) networks, which are part of the TCP/IP protocol suite. Supports management of devices running SNMP agent software by remote administrators using *SNMP manager software*, such as HP OpenView, Novell NMS, IBM NetView, or Sun Net Manager, on remote computers. Devices running SNMP agent software send data from management information bases (*MIBs*) to the SNMP manager software.

On certain Cyclades devices, administrators can enable SNMP to allow a remote administrator to manage the device and can configure the device to send alerts about events of interest. Before enabling SNMP, the administrator needs the following information: The contact person (administrator) of the AlterPath device; the physical location, the *community name* (for SNMP v1, v2c only), IP address or DNS hostname of the *SNMP manager*. The OnBoard supports SNMP v1, v2c, and v3. The SNMP configuration file is located at `/etc/snmp/snmpd.conf`. See also *OID* and *traps*.

SNMP manager

Any computer running SNMP manager software. Also called a network management station or SNMP server.

SNMP manager software

Displays data about managed devices on the console or saves the data in a specified file or database. Some network management programs such as HP OpenView graphically show information about managed devices.

SNMP server (See SNMP manager)

SoL *(*serial over LAN)

Access to the console of a server or other device that supports redirection of serial server data to a dedicated Ethernet port. Permits access to and control of the BIOS and operating system console over the LAN or Internet. Eliminates the need for the device to have a serial port and the need for serial cabling to enable console access. On the OnBoard, once a device's SoL Ethernet port is connected to one of the OnBoard's private Ethernet ports, an authorized user can access the server or a device's console either through the "Device console" or "devconsole" option (available on the *Web Manager*, `rmenush`, or `onbdshell)` or through entering the `devconsole` command with `ssh` on the command line).

SP (service processor)

Ethernet-based management controller on a server, which provides out-of-band management through an interface between the server's administrator and an internal baseboard management controller (BMC) that enables the management features. Management features can include serial console emulation (using Telnet or IPMI), *KVM over IP,* power control, sensor and log information from the server hardware, and virtual media.

SRM (secure rack management)

An out-of-band infrastructure (OOBI) capability delivered by the AlterPath OnBoard that isolates the management ports (emergency service ports) of servers that have *service processors* from the *production network*. Physically consolidates and logically secures the Ethernet connections between the AlterPath OnBoard and the connected service processors. By providing *IP consolidation*, SRM substantially lowers the cost and complexity of deploying service processors. SRM also lowers the security risks of using service processors by providing centralized authentication and user access control, isolating vulnerable service processor protocols from the production network and communicating with authenticated and *authorized users* over the public network using higher-end secure protocols (such as *SSH*, *SSL*, and *HTTPS*).

SSH

Secure shell, developed by SSH Communications Security, Ltd., is a UNIX-based *shell* and protocol that provides strong authentication and secure communications over unsecured channels. Unlike `telnet`, `ftp`, and the `rcp`/`rsh`/`remsh` programs, SSH encrypts everything it sends over the network. Many Cyclades products support SSH version 1 and SSH version 2. Since SSH1 and SSH2 are entirely different, incompatible protocols, it is important when given a choice between enabling one or the other of the two SSH versions to enable the version that is available on the computer being used to access the Cyclades equipment. The OpenSSH (`www.openssh.org`) package is used on the AlterPath OnBoard. THe OnBoard uses the Open SSH version that is certified by the Cryptographic Module Validation (CMV) program run by the U.S. National Institute of Standards (NIST) and the Canadian government's Communications Security Establishment (CSE). Authorized users on the AlterPath OnBoard can enter an OnBoard-specific set of commands such as poweron, poweroff, powercycle when using `ssh` on the command line to perform *service processor* management actions.

SSL (secure sockets layer)

A protocol for transmitting private documents via the Internet. Also used for the type of connection used for transmitting the information. Uses two keys to encrypt data being transferred: a public key and a private or secret key known only to the message receiver. See also *HTTP/HTTPS*.

system event log (See *event log*)

TACACS+ (Terminal Access Controller Access Control System)

An authentication protocol (pronounced *tak-ak_plus*) that provides separate authentication, authorization, and accounting services. Based on TACACS, but completely incompatible with it. Uses the TCP protocol, which is seen by some administrators as a more-reliable protocol than the UDP protocol used by RADIUS. One of many standard authentication protocols supported on Cyclades devices.

trap

An operation started by an SNMP agent in response to an event of interest on a managed-object in a device, which sends an alert to the *SNMP manager*. The administrator of certain Cyclades device can configure which types of events generate trap messages and trap destinations. Also known as SNMP messages or as “PDUs”—protocol data units.

virtual media

Emulates the use of a floppy or CD drive that is physically connected to the remote administrator’s computer to

VPN (virtual private network)

A mechanism enabling two computers to securely transfer information over an otherwise untrusted network through a secure tunnel. Two common options used for VPN are *IPSec* and *PPTP*.

Web Manager

Cyclades' web management interface. The Web Manager runs in supported browsers and allows remote administrators to configure Cyclades products and to enable remote users to access servers and other devices that are connected to Cyclades products. Authorized users can use the Web Manager to access connected devices.

Index

A

access to connected devices
    controlling 3
    planning 11
activity, capturing 4
adding rules for IP filtering chains 65
addressing scheme 55
    planning 98
administrative users 81, 234
    Wizard introduction 82
administrators 74
AH authentication protocol 35
alarm trigger
    email notifications
        to configure 200
    pager notifications
        to configure 198
    SNMP trap notifications
        to configure 196
alarms 4, 51, 53
    configuring 51, 52, 53
ALERT syslog severity level 39
alerts 4
AlterPath PM IPDUs 46, 47
anonymous login, to access Cyclades' ftp server 268
Apache web server 23
application notes 62, 313, 316, 317
authentication 3, 4
    configuring with `cycli` 7
    default method 8
    default type for devices 13
    local fallback option 7
    method 8
    modem 45
    supported methods 5
    supported types for IPSec 33
    type, selecting a default 90
authentication servers 5, 7
    Kerberos, to configure 181
    LDAP, to configure 184
    NIS, to configure 185
    RADIUS, to configure 187
    SMB, to configure 189
    TACACS+, to configure 191
    tasks for configuring 8
authorizations 3
    bypassing in a custom security profile 12
authorized users 3, 46, 47, 311
    managing outlets on IPDUs 46
    tasks to enable VPN for native IP access 37
    VPN configuration tasks 34
autodetect modem access type 44
AUX ports 46, 47

B

backing up configuration files 68
backup partition 373
backups 67
    configuring for added files 70
basic network parameters, configuring 237
baud rate, modem 44
blade manager, connecting 41

bogomips information 261
bond0 42
bonding 41
  configuring 236
boot 372
  configuration fields and options 155
  partitions 373
  to configure 155, 157
boot action, configuring for IPSec VPN 35
boot image 382
  problems, troubleshooting 307, 381
  replacing 307, 372
  saving in compact flash 382
  saving to a flash memory card 383
broadcast IP address 93, 238
bus frequency information 261
buttons
  Save and apply changes 68
  unsaved changes 68

C

callback 43, 46, 74
  connection, used for troubleshooting 304
cautions
  closing PPTP VPN connections to prevent unauthorized access. 39
  risks from not changing administrator's passwords 85
  when adding users in the Wizard 107
  when changing or deleting private subnets 98
  when changing the default `rmenu.sh` menu 49, 51
  when creating a command template 320
  when creating filtering rules 63
certificate signing request, generating 23
certification authorities 23
chains, packet filtering 64
changes to config files, how the OnBoard handles 67
chat string, modem 45
command line
  checking for the PPTP address 39, 354, 364
  using to access the OnBoard 37
command templates 310, 311
  assigning to a new device 165, 316
  assigning to devices, Wizard 106
  creating 312
  `devconsole.default` 106, 321
  `drac.default` 106
  `ilo.default` 106
  `rsa.default` 106
  `rsa.limited.default` 106
  test 312
  when not to use 324
commands
  `commit` 68
  `create_cf` utility 307, 381, 382
  `cycli` utility 7, 9, 46, 63, 68
  `daemon.sh` 306
  `ifconfig` 354
  `ipconfig` 39, 364
  `ipmitool` 316
  `onbdtemplate` utility 312, 316, 319, 320, 325
  `openssl` 23
  `ping` command 318
  `ps` 306
  `restoreconf` 381
  `saveconf` 68, 320
  `ssh` 11, 37, 318
  `telnet` 318
  using for troubleshooting 382

communications
blocked between private Ethernet ports 41
proxied 3
compact flash PCMCIA card, saving the boot image in 382
configsource environment variable 378
configuration 378
backup
`configuration_files_gz`file 68
boot 155
files 67, 68
backed up 373
backup/restore 265
factory default 67, 381, 383
restoring 71
restoring to last saved version 380
saving changesf 68
to restore 380
to restore to factory defaults 381
files changes, persisting after a software upgrade 274
to restore 380
using the Wizrd 84
`configuration_files.gz` backup file 68, 69
console 320, 381
access through dedicated Ethernet ports 54
destination for syslog messages 39
CPU information 261
`create_cf` command 307, 378, 381
`factory_default` option 381
options 382
CRIT syslog severity level 39
`crond` daemon 52
currentimage environment variable 374, 383
curses commands 313
custom security profile 8, 14
bypassing authorizations 12
customizing
command templates 312
expect scripts 312
custom*N* device type 106
Cyclades
ftp server for downloading updated software 268
to download firmware from 119, 269
`cycli` utility 68
`add` command 285, 287
adding/editing `iptables` rules 67
commands 285
`commit` command 288
configuring alarms 51, 52
configuring authentication 7, 63
configuring data buffering 63
configuring IPDU power management 46
configuring modems 43, 44
configuring rules for IP filtering 63
configuring services 17
configuring users 9
`delete` command 288
detecting services starting and stopping 17
example script 62
`exit` command 289, 292
`list` command 291
`quit` command 292
`quit!` command 292
`rename` command 292
`revert` command 293
saving (committing) changes 63, 68
`set` command 293
`shell` command 294
`show` command 289
`version` command 294

D

daemon.sh command, WEB option 306
daemons 52
daisy-chaining IPDUs 46, 117
data buffering 4, 62
  configuring 63
  configuring log file storage 63
  global 62
data filtering, events generating syslog messages 39
date information 261
DEBUG syslog severity level 40
dedicated Ethernet port 53
default
  static IP address 235
default route 51, 93, 235
  specifying 238
  when private subnets are not configured 98
defaults
  configuration
    to restore 380
    to restore as root 381
  configuration files 381, 383
  configuration files, restoring 69, 381
  packet filtering chains 64
Destination Network Address Translation 99, 102
destinations for syslog messages 40
detected devices 258
/dev/hdc PCMCIA slot 1 device name 382
/dev/hde PCMCIA slot 2 device name 382
devconsole.default command template 106, 321
device configuration 310
  unique tasks 310
device console 105
device management 3
device management actions
  event log 313
  power 313
  service processor console 313
device types 105, 311
  differences 312
devices 3
  accessing native IP features on 37
  assigning an authentication method 8
  assigning private subnets 61
  communication with the OnBoard 311
  configuring 53
  configuring new 309–369
  configuring, Wizard 84, 104
  connecting 54
  console access through dedicated Ethernet ports 54
  controlling access to 3
  data buffering for 62
  default authentication method 13
  detected 258
DHCP 17, 93, 235, 238
  configuration for public Ethernet ports, Wizard 94
  configuring for a failover device 94
  configuring for Ethernet ports 236
  configuring for failover device 236
  default route 51, 93, 235
DHCP server 235
dial-in 43, 74
disk space for storing data log files 62
DNAT 99, 102, 311
DNS 234, 237, 238
DNS server 234

document
audience xxix
CD xxxiii
downloads xxxiii
organization xxx
related documentation xxxii
domain name 234, 238
downloading
AlterPath PM firmware 119
documents xxxiii
firmware (software)
AlterPath PM 119, 269
OnBoard firmware 119, 269
release notes 317
DRAC device type 105, 321
DRAC II devices 313
DRAC III/XT devices 313
DRAC IV devices 313
`drac.default` command template 106, 321

E

edit rule for packet filtering chain 65
email notifications 53
EMERG syslog severity level 39
environment variables, currentimage 383
ERROR syslog severity level 40
escape sequence
conventions for xxxiv
device console 320
ESP authentication protocol 35
`/etc/config_files` file
adding a new file to be backed up/restored 70
certificate files pre-added to 24
`/etc/httpd/conf/ssl.key/server.key` file 24
`/etc/menu.ini` login shell configuration file 48
`/etc/onboard_templates.ini` file 320, 321
eth0 42
eth1 42
Ethernet failover, configuring 236
Ethernet PCMCIA card 41
configuration form 139
Ethernet ports 53, 238
introduction 41
configuring, Web Manager 234, 236
private 41
tasks for configuring 42
event log management 313
examples
configuration using the `cycli` utility 62
private subnet configuration 342
two private subnets and VPN 345
virtual network configuration with one private subnet 359
Expect scripts 311
`talk_custom`*N*`.exp` 313
`talk_generic_ipmi.exp` 313
`talk_rsa_I.exp` 313, 325
when a customized one is needed 316
external modems 43

F

factory defaults
configuration 381, 382, 383
restoring 272
to restore 380, 381
configuration files 67, 69
to restore the configuration 381
`factory_default_files.gz` file 69

failover 41, 237
configuration, Wizard 94, 97
configuring 236
files
/etc/onboard_templates.ini file 320, 321
configuration, restoring 71
configuration_files.gz 68, 69
factory_default_files.gz 69
firewall
configuration introduction 63–67
rules, configuring, Web Manager 239
firmware
AlterPath PM
to download from Cyclades 119
configuration file backups before upgrading 269
heading on the Cyclades downloads page 317
image 382
OnBoard
image destination 272
to download from Cyclades 119, 269
upgrade 266
upgrading 267
service processor, tested 316
to download from Cyclades 269
flash memory 62, 272, 378
partitions 381
PCMCIA card 383
configuration form 139
flow control 44
format storage media, while creating a boot image 382
FORWARD packet filtering chain 64
ftp server 269
FTP site, for downloading OnBoard firmware 268
FTPD 18

G

gateway 93
IP address 238
global data buffering 62

H

high-availability 41
host route 51
host settings
Web Manager option 233
host table 242
hosts
adding new, Web Manager 242
configuring network interfaces 233
hot keys, conventions for xxxiv
HTTP 12, 18, 74, 88
HTTPS 12, 17, 23, 74, 88

I

IBM service processors 314
ICMP 12, 18
ifconfig command 39, 42, 354, 364
iLO type devices 105, 321
ilo.default command template 106
ilo.default command template 321
image
destination 272
file 268
software 382
INETD 18
Info menu 258
INFO syslog severity level 40

information
detected devices 258
system 258, 260, 261, 263
system status 258
INPUT packet filtering chain 64
interfaces 234
interfaces, configuring, Web Manager 234
Internet 54
intrusion, reducing risks 85
inverted options for packet filtering 66
IP addresses
broadcast 238
of remote IPSec gateway 35
OnBoard 103
planning 98
IP filtering
introduction 63–67
IPDUs 46
daisy-chaining 46
overcurrent status generating syslog messages 39
planning access to outlets 11
power management 46, 47
IPMI 1.5 105
devices 313
IPMI 2.0 devices 313
IPMI type 106
devices 322
`ipmitool`commands 165, 316
IPSec 4, 17, 247
enabling to support VPN 37
in the moderate security profile 12
VPN connections 35
`iptables` introduction 64–??, 67

K

Kerberos authentication 5, 7, 33, 181
kernel version 261
keys
conventions for hot keys, escape keys, and keyboard shortcuts xxxiv
generated for RSA public keys 35

L

LAN 54
LDAP authentication 5, 7, 33
`/libexec/example_scripts` scripts 8
lightweight directory access protocol 5
Linux 38
commands 382
support for IPSec and PPTP 33
local
administrators, troubleshooting 304
authentication 5
IP address, for configuring a modem card 45
logging, system 4
login 212 FAILED LOGIN error message 304
login shell 48
`rmenush` 48
logins 4, 8
anonymous to `ftp.cyclades.com` 268
modem access type 44
recovering from root login failure 304

M

MAC address 41
machine information 261
Macintosh 38
MacOS X support for IPSec and PPTP 33
management network 41, 53
management, of connected devices 3

message filtering 40
levels, syslog 39
message logging 39–40
/mnt/hda3/backupdirectory 68
modems 43
access options 44
access types 44
configuring 43
external 43
initialization string 45
OnSite, introduction 43–46
PCMCIA card 43, 139
configuration form 139
used for troubleshooting 304
moderate security profile 12, 86
MRU 45
MS-CHAPv2 33
MTU 45, 93, 238
/MRU, value for modem configuration 45

N

native IP 34, 38, 39
access 322
accessing devices 37
navigate, conventions for showing how to xxxiv
net_boot command 374
netmask 103, 238
for IPSec VPN connections 36
network
address 103
boot 378
saving image to flash memory 272
configuration 318
configuring basic parameters, Web Manager 237
network interfaces
configuring 233, 234
configuring a default route 51, 93, 235
configuring, Web Manager 234
configuring, Wizard 84, 91
network route 51
network services 3
NIS authentication server
to configure 184, 185, 187, 189, 191, 196, 198, 200, 202
NOTICE syslog severity level 40
notifications 4
configuring 53
NTP 18

O

onbdtemplate utility 312, 316, 319, 320, 325
OnBoard
administrator 312
configuring a default route 51, 93, 235
data buffering on 62
features overview 3
flash memory 62
granting access to VPN connections 34
how device communications are managed 311
IP address for the public interface 38
restart 266
SNMP on 31
supported devices and firmware levels 311
system events generating syslog messages 39
understanding authentication on 4
unique device configuration requirements 310
unique security features 3

open security profile 13
`openssl` utility 23
OpenSWAN 33
operating system, upgrading 267
organization, document xxx
outlets, managing 46
OUTPUT packet filtering chain 64
overcurrent alerts 40

P

packet filtering 63
  introduction 63–67
  on the OnBoard 63
  overview 64
  rules 64
pager notifications 53
partitions 381, 382
  rebuilding 382
passwords 74
  admin, changing from default 85
PCMCIA cards 382
  flash memory, for saving a boot image 383
  modem 43
    to begin configuring 142
    to configure 142, 147, 149, 151
  slots, device names 382
periodic checks of sensor readings, configuring 53
`ping` command 318
planning
  access to connected devices 11
  device IP addresses 98
  user access to devices and outlets 11
power management
  commands 312, 318, 325
  configuring 46
  device 313
  on IBM servers using RSA II cards 314
power on 312
power supply state 261
PPP 4, 10, 45, 74
  configuring options 46
  modem access type 44
  options 46
PPP/PPTP access 108, 171
PPTP 4, 10, 12, 18, 33, 34
  client 33, 38, 353
  password 38
  VPN connections 38
pptp-linux 33
preshared key (PSK) 33
primary Ethernet port 53
  configuring, Web Manager 234
priv0 41, 339
private Ethernet ports 41, 53
private IP addresses, configuring 336
private network 3, 41
private subnets 310, 311
  caution when changing or deleting 98
  configuration example 342, 345
  configuring, Wizard 84, 98
  parameters for configuring 100
production network 53
protocols, vulnerabilities not exposed on public network 3
proxied communications 3
`ps` command 306
PSK (preshared key) 33
public key
  SSL 23
  SSL certificate request 24
public network 3, 41

PVR 261

R

RADIUS authentication 6, 7, 33
RAM 67, 381
    saving an image to flash 272
RAMDISK 274, 374, 378
reboot 274
    persistence of configuration file changes 67
recovering from root login failure 304
release notes 63, 311, 317
remote
    administrators 4
        troubleshooting 304
    IP address
        for modem 45
removable flash 374
requirements
    for device configuration 310
    for enabling VPN 247
restart 274
    OnBoard 266
restoration
    configuring for added files 70
    of configuration files 380
`restoreconf` command
    factory_default option 381
    options 384
restoring
    backed up configuration files 67
    configuration files 71, 265
    factory default configuration files 67, 69
revision, CPU, information 261
`rmenush` login shell, configuring 48
root user 51
    cannot log in 304
routes, default, configuring for the OnBoard 51, 93, 235
routing
    for the OnBoard, understanding 51
    specifying the OnBoard's default route 51, 93, 235
RPC 12, 18
RSA I type devices 313, 325
RSA II type devices 105, 312, 314, 321, 325
RSA public keys 33, 35
`rsa.default` command template 106, 318, 321, 325
`rsa.limited.default` command template 106, 318, 321, 325
`RSA_I.txt` application note 313
rules
    configuring for packet filtering 63
    hidden, for packet filtering 64
    packet filtering 64

S

save and apply changes
    button 68
    `cycli` 68
Save button
    on the Mgmt -> Backup/restore screen 68
`saveconf` command 320, 380
    backing up configuration changes 68
saving configuration file changes 68
screens, conventions for showing how to navigate to xxxiv
scripts, configuring backups for 70
secondary Ethernet port 41
    configuring, Web Manager 234
secured security profile 13, 88

security
changing admin user password 85
features unique to OnBoard 3
isolating devices from the public network 41
policies, enforcing with a security profile 12
security profiles 3
custom 8
customizable services/features 14
customizing in the WIzard 90
effect on authorizations 12
moderate 86
moderate, services/features 12
open 89
open, services/features 13
secured 88
secured, services/features 13
selecting or configuring, Wizard 85
selecting or customizing, Wizard 84
Web Manager Wizard configuration dialog 86
self-signed certificates 23
sensor alarms 40, 52
configuring 51, 52
to configure 202
sensor data management on IBM servers with RSA II cards 314
sensors events generating syslog messages 39
servers
authentication
LDAP, configuring 184
NIS, configuring 185
RADIUS, configuring 187
SMB, configuring 189
TACACS+, configuring 191
syslog 40
service processors 41, 53, 54
console 313, 318
hiding vulnerable protocols used by 3
management features 3
power management 46, 47
services 3
controlled by security profiles 12
session status 258
shared secret 35
SMB authentication 6
SNMP 12, 18
configuration tasks 31
trap notifications 53
v1, v2, v3 30
software
AlterPath PM
to download from Cyclades 119
heading on the Cyclades downloads page 317
OnBoard
image destination 272
to download from Cyclades 119, 269
upgrade 266
upgrading 267
onfiguration file backups before upgrading 269
software image 382
file 268
software upgrade
configuration 274
retaining configuration file changes 67
software, updated
downloading from Cyclades 268
SPs (service processors) 41, 53, 54
console 313, 318
hiding vulnerable protocols used by 3
management features 3
power management 46, 47

SSH 12, 18, 381
encryption 3
`ssh` command 11, 37, 39, 47, 318, 354, 364
SSL 23
certificate requirements 23
static IP address 33, 237, 238
configuration for primary/secondary Ethernet ports, Wizard 95
configuring for Ethernet ports, Web Manager 236
subnets
configuring, Wizard 84, 98
for IPSec VPN connections 36
supporting multiple 102
syslog 18, 39
introduction 39–??
message filtering levels 39
message notifications 53
servers 39, 40
severity levels 39
syslog servers 40
syslogd 40
syslogging 40
servers 40
system information 258, 260, 261, 263

T

TACACS+ authentication 6, 33
`talk_custom`*N*`.exp` Expect script 313
`talk_generic_ipmi.exp` Expect script 313
`talk_rsa_I.exp` Expect script 313, 325
tasks
configuration using the Wizard 84
device configuration 310
for administering packet filtering 66
for assigning a command template to a device 316
for backing up/restoring configuration files 71
for basic configuration, Wizard 82
for configuring
authentication 8
Ethernet ports 42
IPSec VPN 37
modems 43
native IP access 37
power management 47
PPTP VPN connections 38
SNMP 31
syslog 40
users and groups 11
VPN 34, 37
for enabling PPTP connections and native IP 38
for planning access to connected devices 11
performed under Web Manager Mgmt 265
performed using the Wizard 81
Telnet 12, 18, 381
`telnet` command 318
Terminal Access Controller Access Control System authentication 6
terminal emulator 43
TFTP boot server 272, 378, 379
trap notifications 53
triggers, for notifications 53

troubleshooting 303–307, 378
boot image problems 307, 381
connection methods 304
device configuration 312
list of topics 303
network failure 304
troubleshooting boot 372
tunnel 37
typographical conventions xxxiii

U

U-boot monitor mode 379
U-Boot, details 307, 372
UNIX-based servers 40
unsaved changes button 68
Unsaved changes light 87
upgrading OnBoard firmware 266, 267
uptime information 261
username for Cyclades ftp site 268
users 8
activity, capturing 4
configuring for power management 47
configuring, Wizard 84, 107
planning device and IPDU outlet access 11
users and groups authorizations 3
`/usr/bin/rmenush` login shell
configuring 48

V

`/var/log/console/`*`devicename`* log 62
vendor, CPU, information 261
virtual IP addresses 102, 310, 311
virtual network 37, 102, 311
configuration, Wizard 99
VPN
configuration example 345
configuration tasks 34
connection 38
introduction 32–39
overview 64

W

WARNING syslog severity level 40
Web Manager
conventions for showing how to navigate to screens xxxiv
restarting 306
Wizard 81
web server 23
Windows 38
support for IPSec and PPTP 33
wireless PCMCIA card configuration screen 139
Wizard 81–109
menu options 82

X

X.509 certificates 33