



Avocent®

Cyclades® OnBoard

Installer/Administrator Guide



FCC Warning Statement

The Cyclades OnBoard service processor manager has been tested and found to comply with the limits for Class A digital devices, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the Installation & Service Manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user is required to correct the problem at his or her own expense.

Safety and EMC Approvals and Markings

C-Tick, ICES 003, FCC Part 15 Class A, CE



Cyclades[®] OnBoard Service Processor Manager Installer and Administrator Guide

Avocent, the Avocent logo, The Power of Being There and Cyclades are registered trademarks of Avocent Corporation or its affiliates. All other marks are the property of their respective owners.

© 2006 Avocent Corporation. All rights reserved. 590-663-501A

**Instructions**

This symbol is intended to alert the user to the presence of important operating and maintenance (servicing) instructions in the literature accompanying the appliance.

**Dangerous Voltage**

This symbol is intended to alert the user to the presence of uninsulated dangerous voltage within the product's enclosure that may be of sufficient magnitude to constitute a risk of electric shock to persons.

**Power On**

This symbol indicates the principal on/off switch is in the on position.

**Power Off**

This symbol indicates the principal on/off switch is in the off position.

**Protective Grounding Terminal**

This symbol indicates a terminal which must be connected to earth ground prior to making any other connections to the equipment.

TABLE OF CONTENTS

List of Figures	xi
List of Tables	xv
Chapter 1: Installation Introduction	1
<i>OnBoard Appliance Connectors.....</i>	<i>1</i>
<i>OnBoard Appliance Models.....</i>	<i>3</i>
<i>LEDs</i>	<i>3</i>
<i>PCMCIA Card Slots.....</i>	<i>5</i>
<i>Modem Types and Options</i>	<i>5</i>
<i>Console Port</i>	<i>6</i>
Chapter 2: Basic Installation Procedures	7
<i>Getting Started.....</i>	<i>8</i>
<i>Supplied with the OnBoard Appliance.....</i>	<i>9</i>
<i>Rack Mounting the Cyclades OnBoard SP Manager</i>	<i>9</i>
<i>Making Public Ethernet Connections</i>	<i>10</i>
<i>Connecting Devices</i>	<i>11</i>
<i>Connecting to a Power Source and Powering Up.....</i>	<i>11</i>
<i>Methods for Enabling Web Manager Access.....</i>	<i>13</i>
<i>Connecting a Terminal to Configure Basic Network Parameters</i>	<i>14</i>
<i>Enabling Access to the Web Manager</i>	<i>14</i>
<i>Changing the root User's Password.....</i>	<i>17</i>
<i>Selecting a Security Profile, Adding Users and Configuring Devices Using the Web Manager</i>	<i>17</i>
Chapter 3: Advanced Installation Topics and Tasks	19
<i>Installing PCMCIA Cards in the Front Card Slots</i>	<i>19</i>
<i>Connecting an External Modem to the AUX Port</i>	<i>20</i>
<i>Connecting One or More IPDUs to the AUX Port</i>	<i>21</i>
Chapter 4: Introduction for Administrative Users.....	23
<i>Overview of OnBoard Appliance Features for Administrators</i>	<i>23</i>
<i>OnBoard Appliance Authentication Options</i>	<i>24</i>
<i>One-time Password Authentication on the OnBoard Appliance</i>	<i>28</i>

<i>OnBoard User and Group Configuration Options</i>	29
<i>Configuring user and group accounts</i>	29
<i>OnBoard Appliance Security Profiles</i>	30
<i>OnBoard Appliance Services</i>	32
<i>Telnet on the OnBoard Appliance</i>	33
<i>Telnet service configuration</i>	33
<i>Telnet client configuration</i>	33
<i>Telnet configuration tasks</i>	33
<i>HTTPS on the OnBoard Appliance</i>	34
<i>DHCP on the OnBoard Appliance</i>	34
<i>DHCP client</i>	34
<i>DHCP server</i>	34
<i>SNMP on the OnBoard Appliance</i>	35
<i>VPN on the OnBoard Appliance</i>	39
<i>Message Logging (With Syslog) on the OnBoard Appliance</i>	39
<i>Message filtering levels</i>	40
<i>Syslog servers</i>	40
<i>Tasks for configuring syslog messages</i>	40
<i>Ethernet Ports on the OnBoard Appliance</i>	41
<i>Private Ethernet ports</i>	41
<i>Public Ethernet ports</i>	41
<i>Dial-in and Callback Access to the OnBoard Appliance</i>	42
<i>Power Management Options on the OnBoard Appliance</i>	44
<i>Adding Options to the User's Console Login Menu</i>	44
<i>Routing on the OnBoard Appliance</i>	44
<i>Tasks for configuring routes</i>	45
<i>OnBoard Appliance Notifications</i>	45
<i>OnBoard Appliance Sensor Alarms</i>	46
<i>Device Configuration</i>	47
<i>Preparing an addressing scheme</i>	48
<i>Parameters for configuring devices</i>	50
<i>Private Subnets on the OnBoard Appliance</i>	51
<i>Tasks for Configuring IP Addresses</i>	52
<i>Example and Demo Scripts</i>	52
<i>Data Buffering on the OnBoard Appliance</i>	52

<i>Enabling data buffering</i>	52
<i>Configuring where buffered data is stored</i>	52
<i>Firewall/Packet Filtering on the OnBoard Appliance</i>	53
<i>Chains</i>	53
<i>Rules</i>	53
<i>Add rule and edit rule options</i>	54
<i>Tasks for administering packet filtering</i>	55
<i>How Configuration Changes Are Handled</i>	55
Chapter 5: Administration Tasks Not Performed in the Web Manager	57
<i>Configuring Storage of Buffered Data</i>	57
<i>Using MindTerm to Create an SSH Tunnel</i>	59
<i>Specifying the Location for the OTP Databases</i>	60
<i>How Users are Registered with OTP and Obtain OTP Passwords</i>	62
<i>Configuring SSH or Bidilink Instead of Telnet for Device Connections</i>	65
<i>Replacing the Self-Signed Certificate With an SSL Certificate for HTTPS</i>	66
<i>Configuring the DHCP Server</i>	68
<i>Configuring VPN Connections</i>	70
<i>VPN client system requirements and limitations</i>	71
<i>IPSec VPN connections</i>	71
<i>PPTP VPN connections</i>	73
<i>Configuring Dial-ins Using cycli</i>	74
<i>Configuring the User's Console Login Menu</i>	78
<i>Configuring Routes With cycli</i>	79
<i>Saving Configuration Changes</i>	81
<i>Backing Up Configuration Files</i>	81
<i>Restoring Backed Up Configuration Files</i>	82
<i>Restoring Factory Default Configuration Files</i>	82
<i>Adding New Files to Be Backed Up and Restored</i>	82
<i>Changing Web Manager Time-outs</i>	83
<i>Changing the Sort Order of Device Listings</i>	83
<i>Configuring Groups for Use with Authentication Servers</i>	84
<i>Configuring group authorization for LDAP authentication</i>	84
<i>Configuring group authorization for RADIUS authentication</i>	86
<i>Configuring group authorization for TACACS+ authentication</i>	89

Chapter 6: Using the Web Manager.....	93
<i>Logging Into the Web Manager for Administrative Users</i>	<i>93</i>
<i>Features of administrative users' screens</i>	<i>94</i>
<i>Web Manager Wizard</i>	<i>95</i>
<i>Using the Wizard</i>	<i>96</i>
<i>Changing the administrative user's password</i>	<i>97</i>
<i>Selecting a security profile</i>	<i>98</i>
<i>Configuring network interfaces</i>	<i>99</i>
<i>Configuring private subnets and virtual addresses</i>	<i>103</i>
<i>Configuring private subnets</i>	<i>104</i>
<i>Configuring a virtual network</i>	<i>105</i>
<i>Configuring devices</i>	<i>106</i>
<i>Configuring regular users</i>	<i>108</i>
<i>Web Manager Access Menu Options for Administrative Users</i>	<i>109</i>
<i>Accessing the OnBoard appliance console through the Web Manager</i>	<i>110</i>
<i>Upgrading IPDU software</i>	<i>111</i>
<i>Web Manager settings menu options</i>	<i>114</i>
<i>Configuring the AUX port</i>	<i>115</i>
<i>Modem access type menu options</i>	<i>116</i>
<i>Configuring IPDU Power Management</i>	<i>119</i>
<i>Configuring over current protection for an IPDU</i>	<i>120</i>
<i>Configuring users to manage power outlets on a connected IPDU</i>	<i>121</i>
<i>Configuring names and power up intervals for outlets on a connected IPDU</i>	<i>122</i>
<i>Configuring PCMCIA cards</i>	<i>123</i>
<i>Configuring system date and time</i>	<i>132</i>
<i>Configuring the boot file location</i>	<i>133</i>
<i>Configuring outbound email</i>	<i>135</i>
<i>Configuring an alternate help file location</i>	<i>136</i>
<i>Web Manager Config Menu Options</i>	<i>137</i>
<i>Configuring devices</i>	<i>138</i>
<i>Adding a device</i>	<i>139</i>
<i>Configuring Users and Groups</i>	<i>140</i>
<i>Configuring users</i>	<i>140</i>
<i>Configuring groups</i>	<i>140</i>

<i>Configuring device groups</i>	143
<i>Configuring Authentication</i>	144
<i>Configuring authentication servers</i>	144
<i>Configuring a Kerberos authentication server</i>	145
<i>Configuring an LDAP authentication server</i>	146
<i>Configuring a NIS authentication server</i>	147
<i>Configuring a RADIUS authentication server</i>	148
<i>Configuring an SMB authentication server</i>	149
<i>Configuring a TACACS+ authentication server</i>	150
<i>Prerequisites for a TACACS+ server configuration</i>	150
<i>Configuring an authentication method for the OnBoard appliance</i>	151
<i>Configuring Notifications</i>	152
<i>Configuring SNMP trap notifications</i>	153
<i>Configuring pager notifications</i>	154
<i>Configuring email notifications</i>	155
<i>Configuring Sensor Alarms</i>	155
<i>Configuring a syslog message sensor alarm action</i>	157
<i>Configuring the SNMP trap sensor alarm action</i>	157
<i>Configuring a pager sensor alarm action</i>	159
<i>Configuring an email sensor alarm action</i>	160
<i>Configuring SNMP</i>	161
<i>Configuring SNMP for devices</i>	162
<i>Configuring device SNMP settings</i>	162
<i>Configuring SNMP device access settings</i>	163
<i>Configuring SNMP trap forwarding for devices</i>	166
<i>Configuring Logging of System Messages (Syslogs)</i>	166
<i>Syslog destination</i>	167
<i>Configuring the Event Log Backend</i>	168
<i>Selecting or Configuring a Security Profile</i>	169
<i>Web Manager Network Menu Options</i>	170
<i>Configuring network interfaces</i>	171
<i>Configuring firewall rules for packet filtering</i>	174
<i>Configuring hosts</i>	177
<i>Configuring static routes</i>	178
<i>Configuring VPN connections</i>	179

<i>Configuring private subnets and virtual networks</i>	182
<i>Web Manager Info Menu Options</i>	186
<i>Viewing status information about active sessions</i>	187
<i>Viewing system information</i>	188
<i>Viewing information about detected devices</i>	188
<i>Web Manager Mgmt Menu Options</i>	189
<i>Backing up or restoring configuration files</i>	190
<i>Upgrading OnBoard appliance firmware</i>	190
<i>Restarting the OnBoard appliance</i>	195
Chapter 7: Using the cycli Utility	197
<i>cycli Utility Overview</i>	197
<i>Execution Modes</i>	198
<i>Command line mode</i>	198
<i>Interactive mode</i>	198
<i>Batch mode</i>	198
<i>cycli Options</i>	199
<i>cycli Parameters and Arguments</i>	199
<i>Entering values with parameters</i>	200
<i>Entering a command in interactive mode</i>	200
<i>Entering a command in command code</i>	201
<i>Entering a command in batch mode</i>	201
<i>Autocompletion</i>	202
<i>cycli Commands</i>	204
<i>add</i>	204
<i>cd</i>	210
<i>commit</i>	211
<i>delete</i>	211
<i>get show</i>	211
<i>list</i>	213
<i>quit exit</i>	214
<i>quit!</i>	214
<i>rename</i>	214
<i>revert</i>	214
<i>set</i>	215

<i>shell</i>	215
<i>version</i>	216
<i>Summary of How to Configure the Top Level Parameters</i>	216
Appendices	223
<i>Appendix A: Troubleshooting</i>	223
<i>Appendix B: Technical Specifications</i>	226
<i>Appendix C: Safety Information</i>	228
<i>Appendix D: Device Configuration</i>	230
<i>Appendix E: Advanced Boot and Backup Configuration</i>	272
<i>Appendix F: Technical Support</i>	280
Index	283

LIST OF FIGURES

<i>Figure 1.1: OnBoard Appliance Front With PCMCIA Card Slots and Two AC Power Inlets</i>	2
<i>Figure 1.2: OnBoard Front With PCMCIA Card Slots and Two DC Terminal Blocks</i>	2
<i>Figure 1.3: OnBoard Appliance Back With Ethernet, AUX, and Console Ports</i>	2
<i>Figure 1.4: LEDs for Private Ethernet Ports</i>	3
<i>Figure 1.5: LEDs for AUX, Public Ethernet and Console Ports (Back)</i>	4
<i>Figure 1.6: PCMCIA Slots on the OnBoard Appliance Front</i>	5
<i>Figure 2.1: Basic Installation Connections Illustrated</i>	7
<i>Figure 2.2: Bracket Mounting Holes on the OnBoard appliance's Right Side</i>	9
<i>Figure 2.3: Wiring the DC Power Terminal to Positive and Negative DC Power Connectors</i>	12
<i>Figure 2.4: Wiring the DC Power Terminal to Ground</i>	13
<i>Figure 3.1: Connecting an External Modem to the AUX Port and to the Telephone Network</i>	20
<i>Figure 4.1: Recommended Device Configuration</i>	48
<i>Figure 4.2: IP Addressing Example</i>	49
<i>Figure 5.1: MindTerm Basic Tunnels Setup Dialog</i>	60
<i>Figure 6.1: Administrative User Options on the Web Manager</i>	94
<i>Figure 6.2: Example Dialog: Devices Configuration in Wizard Mode</i>	95
<i>Figure 6.3: OnBoard Appliance Configuration Wizard Screen</i>	96
<i>Figure 6.4: Wizard Confirm Changes Screen</i>	97
<i>Figure 6.5: Wizard Configure Administrator Password Screen</i>	97
<i>Figure 6.6: Network Interfaces Screen</i>	99
<i>Figure 6.7: Configure Failover Device Screen</i>	101
<i>Figure 6.8: Configure Primary Ethernet Connection Screen: Static IP</i>	102
<i>Figure 6.9: Configure Subnets Screen</i>	103
<i>Figure 6.10: Network-Private Subnets: Add Subnet Dialog</i>	104
<i>Figure 6.11: Configure Devices Screen</i>	107
<i>Figure 6.12: Add New Device and Edit Dialog</i>	107
<i>Figure 6.13: Add a Regular User Screen</i>	108
<i>Figure 6.14: Fields for Setting a PPP or PPTP Password</i>	108
<i>Figure 6.15: Access Menu Options</i>	109
<i>Figure 6.16: IPDU Software Upgrade Screen</i>	111
<i>Figure 6.17: Upgrade Button on the IPDU Software Upgrade Screen</i>	111

<i>Figure 6.18: IPDU Software Upgrade Screen With Upgraded Software</i>	<i>112</i>
<i>Figure 6.19: Settings-AUX Port-Power Management.....</i>	<i>115</i>
<i>Figure 6.20: Settings-AUX Port -Modem.....</i>	<i>116</i>
<i>Figure 6.21: Callback Number Field Under Settings-AUX Port -Modem.....</i>	<i>116</i>
<i>Figure 6.22: Settings-AUX Port -Modem -PPP</i>	<i>117</i>
<i>Figure 6.23: Settings-AUX Port -Modem -Login</i>	<i>117</i>
<i>Figure 6.24: Settings-AUX Port-Modem-OTP</i>	<i>118</i>
<i>Figure 6.25: Settings-IPDU Screen.....</i>	<i>119</i>
<i>Figure 6.26: Settings-IPDU Screen Without AUX Port Configuration.....</i>	<i>119</i>
<i>Figure 6.27: Settings IPDU General Screen.....</i>	<i>120</i>
<i>Figure 6.28: Settings IPDU General Screen.....</i>	<i>120</i>
<i>Figure 6.29: Settings-IPDU-Users Screen</i>	<i>121</i>
<i>Figure 6.30: Settings-IPDU-Users-Add User Dialog</i>	<i>122</i>
<i>Figure 6.31: Settings-IPDU-Outlets Screen.....</i>	<i>123</i>
<i>Figure 6.32: Settings-PCMCIA-Configure Dialog-Modem or GSM.....</i>	<i>125</i>
<i>Figure 6.33: Settings-PCMCIA-Configure Modem or GSM> Login.....</i>	<i>126</i>
<i>Figure 6.34: Settings-PCMCIA-Configure Modem or GSM-PPP</i>	<i>126</i>
<i>Figure 6.35: Settings-PCMCIA-Configure Modem or GSM-OTP</i>	<i>127</i>
<i>Figure 6.36: Settings-PCMCIA-Configure-Ethernet or Wireless LAN-DHCP.....</i>	<i>128</i>
<i>Figure 6.37: Settings-PCMCIA-Configure Ethernet Dialog-Without DHCP</i>	<i>129</i>
<i>Figure 6.38: Settings-PCMCIA-Configure-Ethernet or Wireless LAN-DHCP.....</i>	<i>130</i>
<i>Figure 6.39: Settings-PCMCIA-Configure Wireless LAN Dialog Without DHCP.....</i>	<i>130</i>
<i>Figure 6.40: Settings-PCMCIA-Configure Flash Dialog: Mount Option Unchecked.....</i>	<i>131</i>
<i>Figure 6.41: Settings-Date/time Screen.....</i>	<i>132</i>
<i>Figure 6.42: -Boot Configuration Screen.....</i>	<i>133</i>
<i>Figure 6.43: Settings-Outbound Email Screen.....</i>	<i>136</i>
<i>Figure 6.44: Settings-Help Screen.....</i>	<i>136</i>
<i>Figure 6.45: Config-Devices Screen</i>	<i>138</i>
<i>Figure 6.46: Config-Users and Groups Screen.....</i>	<i>140</i>
<i>Figure 6.47: Config-Device Groups Screen.....</i>	<i>143</i>
<i>Figure 6.48: Default Config-Unit Authentication Screen</i>	<i>151</i>
<i>Figure 6.49: Default Config-Notifications Screen</i>	<i>152</i>
<i>Figure 6.50: Default Config-Sensor Alarms Screen.....</i>	<i>156</i>
<i>Figure 6.51: Default Config-Sensor Alarms Screen.....</i>	<i>156</i>
<i>Figure 6.52: Config-Sensor Alarms Syslog Message Fields</i>	<i>157</i>

<i>Figure 6.53: Config-Sensor Alarms SNMP Trap Fields for V1 and V2c</i>	157
<i>Figure 6.54: Config-Sensor Alarms SNMP Trap Fields for V3</i>	158
<i>Figure 6.55: Config-Sensor Alarms Pager Message Fields</i>	159
<i>Figure 6.56: Config-Sensor Alarms Email Message Fields</i>	160
<i>Figure 6.57: Config-SNMP Configuration Screen</i>	161
<i>Figure 6.58: Config-SNMP: Edit OnBoard appliance Information Settings</i>	161
<i>Figure 6.59: Device SNMP Settings Screen</i>	162
<i>Figure 6.60: Config-SNMP: Device SNMP Access Dialog With V1 or V2c Selected</i>	163
<i>Figure 6.61: Config-SNMP: Device SNMP Access Dialog With V3 Selected</i>	163
<i>Figure 6.62: Config-SNMP: Add Trap Forwarding</i>	166
<i>Figure 6.63: Config-Event Log Backend: Edit Dialog</i>	168
<i>Figure 6.64: Network Menu Options</i>	170
<i>Figure 6.65: Network-Host Settings Screen</i>	171
<i>Figure 6.66: Network-Host Settings Screen With Failover Enabled</i>	172
<i>Figure 6.67: Network-Host Settings Screen, Both Interfaces Enabled and DHCP Disabled</i>	173
<i>Figure 6.68: Network-Firewall Screen</i>	175
<i>Figure 6.69: Network-Firewall: Add Rule Dialog</i>	176
<i>Figure 6.70: Network-Host Table Screen</i>	177
<i>Figure 6.71: Network-Host Table: Add New Host Dialog</i>	177
<i>Figure 6.72: Network-Static Routes Screen</i>	178
<i>Figure 6.73: Network-VPN Connections Screen</i>	180
<i>Figure 6.74: IPSec VPN Connection Configuration Dialog</i>	180
<i>Figure 6.75: PPTP VPN Connection Configuration Fields</i>	181
<i>Figure 6.76: Network-Private Subnets Screen</i>	183
<i>Figure 6.77: Network-Private Subnets: Add Subnet Dialog</i>	184
<i>Figure 6.78: Info Menu Options</i>	186
<i>Figure 6.79: Info-Session Status Screen</i>	187
<i>Figure 6.80: Info-System Information Screen</i>	188
<i>Figure 6.81: Info-Detected Devices Screen</i>	188
<i>Figure 6.82: Mgmt Options</i>	189
<i>Figure 6.83: Mgmt-Backup/restore Screen</i>	190
<i>Figure 6.84: Mgmt-Firmware Upgrade Screen</i>	191
<i>Figure 6.85: Mgmt-Firmware Upgrade Screen With Net Boot Message</i>	194
<i>Figure 6.86: Mgmt-Restart Screen</i>	195
<i>Figure 7.1: Example Branch in the cycli Parameter Tree</i>	199

<i>Figure D.1: Example 1: Private Subnet</i>	<i>252</i>
<i>Figure D.2: Private Subnet Configuration Example</i>	<i>253</i>
<i>Figure D.3: Example 1: Device Configuration Example</i>	<i>253</i>
<i>Figure D.4: Example 2: Two Private Subnets</i>	<i>255</i>
<i>Figure D.5: Example 2: Values for Configuring Two Subnets.....</i>	<i>256</i>
<i>Figure D.6: Example 2: Four Devices Configured on the Config -Devices Screen.....</i>	<i>257</i>
<i>Figure D.7: Example 2: Configuring a User Account for Native IP Access to All Devices</i>	<i>257</i>
<i>Figure D.9: Example 2: Configuring IPSec Access to a Private Subnet and Two Devices.....</i>	<i>259</i>
<i>Figure D.10: PPTP VPN Configuration Example: Address Pools</i>	<i>260</i>
<i>Figure D.11: PPTP User Configuration Example</i>	<i>261</i>
<i>Figure D.13: Example 3: Virtual Network Configuration</i>	<i>265</i>
<i>Figure D.14: Example Values for Configuring Two Private Subnets With a Virtual Network.....</i>	<i>266</i>
<i>Figure D.15: Example 1: Device Configuration Example</i>	<i>267</i>
<i>Figure D.16: Access-Devices Screen With Virtual IP Addresses.....</i>	<i>267</i>
<i>Figure D.17: Example 3: IPSec Connection Configuration for Access to sub1 Private Subnet and sp1 and sp2 Devices.....</i>	<i>268</i>
<i>Figure E.1: Boot Partitions</i>	<i>273</i>

LIST OF TABLES

<i>Table 1.1: OnBoard Appliance Models</i>	3
<i>Table 1.2: LED Descriptions</i>	4
<i>Table 2.1: Tasks for Basic Installation</i>	8
<i>Table 2.2: Methods for Enabling Web Manager Access</i>	13
<i>Table 4.1: Security Features and Where Documented</i>	23
<i>Table 4.2: Supported Authentication Types</i>	25
<i>Table 4.3: Tasks for Configuring Authentication</i>	27
<i>Table 4.4: Tasks for Configuring OTP Authentication for Dial-ins</i>	28
<i>Table 4.5: User Configuration Settings</i>	29
<i>Table 4.6: User and Group Configuration Tasks</i>	30
<i>Table 4.7: Default Security Profile Services/ Features</i>	31
<i>Table 4.8: Services That Require Additional Configuration</i>	32
<i>Table 4.9: Tasks for Changing the Default Telnet Configuration</i>	33
<i>Table 4.10: Values for Configuring SNMP</i>	36
<i>Table 4.11: Values for Configuring an SNMP Trap Notification</i>	38
<i>Table 4.12: Values for Configuring an SNMP Trap Notification</i>	38
<i>Table 4.13: Tasks for Configuring SNMP</i>	39
<i>Table 4.14: Tasks for Configuring Syslog Messages</i>	40
<i>Table 4.15: Tasks for Configuring Dial-ins and Installing Modems</i>	42
<i>Table 4.16: Modem and Phone Card Field and Menu Options</i>	43
<i>Table 4.17: Tasks for Configuring Power Management</i>	44
<i>Table 4.18: Tasks for Configuring Routes</i>	45
<i>Table 4.19: Values for Configuring Sensor Alarms</i>	46
<i>Table 4.20: Device Configuration Parameters</i>	50
<i>Table 4.21: Filter Options for Packet Filtering Rules</i>	54
<i>Table 4.22: Tasks for Configuring Packet Filtering (Firewall) Rules</i>	55

<i>Table 4.23: Tasks for Saving Changes, Backing Up and Restoring Configuration Files</i>	<i>56</i>
<i>Table 5.1: Configuration Files Used in Data Buffering.....</i>	<i>57</i>
<i>Table 5.2: Required Information When Creating a SSL Certificate Request.....</i>	<i>67</i>
<i>Table 5.3: Tasks for Configuring VPN Connections</i>	<i>70</i>
<i>Table 5.4: VPN Client System Requirements and Limitations</i>	<i>71</i>
<i>Table 5.5: IPSec VPN Configuration Information for Administrators and Users</i>	<i>71</i>
<i>Table 5.6: Methods for Configuring the TACACS+ Authentication Server for Raw Access</i>	<i>89</i>
<i>Table 6.1: Network Interfaces Configuration Values.....</i>	<i>99</i>
<i>Table 6.2: Ethernet Port Settings</i>	<i>100</i>
<i>Table 6.3: Fields on the Private Subnet Configuration Dialog.....</i>	<i>104</i>
<i>Table 6.4: Fields on the Private Subnet Virtual Network Configuration Dialog.....</i>	<i>106</i>
<i>Table 6.5: Options Under Settings</i>	<i>114</i>
<i>Table 6.6: Options Under Settings-IPDU.....</i>	<i>119</i>
<i>Table 6.7: PCMCIA Action Buttons</i>	<i>124</i>
<i>Table 6.8: Boot Configuration Fields and Options</i>	<i>135</i>
<i>Table 6.9: Options Under Config</i>	<i>137</i>
<i>Table 6.10: Tasks for Authentication Configuration.....</i>	<i>144</i>
<i>Table 6.11: Values for Configuring Any Type of Notification.....</i>	<i>152</i>
<i>Table 6.12: Fields for Configuring a Pager Notification.....</i>	<i>154</i>
<i>Table 6.13: Fields for Configuring an Email Notification</i>	<i>155</i>
<i>Table 6.14: Fields for Configuring Pager Sensor Alarms.....</i>	<i>159</i>
<i>Table 6.15: Fields for Configuring Email Sensor Alarms.....</i>	<i>160</i>
<i>Table 6.16: Network Interfaces Configuration Values.....</i>	<i>171</i>
<i>Table 6.17: Fields and Menus for Configuring Static Routes</i>	<i>178</i>
<i>Table 6.18: Fields for Configuring a PPTP Profile</i>	<i>182</i>
<i>Table 6.19: Fields on the Private Subnet Configuration Dialog.....</i>	<i>183</i>
<i>Table 6.20: Fields on the Private Subnet Virtual Network Configuration Dialog.....</i>	<i>184</i>
<i>Table 6.21: Options Under Info.....</i>	<i>186</i>
<i>Table 6.22: Information on the Info-Session Status Screen.....</i>	<i>187</i>

<i>Table 6.23: Information on the Info-Detected Devices Screen.....</i>	<i>188</i>
<i>Table 6.24: Firmware Upgrade Screen Fields.....</i>	<i>191</i>
<i>Table 7.1: cycli Utility Options.....</i>	<i>199</i>
<i>Table 7.2: Parameters That Work With the cycli add Command.....</i>	<i>206</i>
<i>Table 7.3: Top Level cycli Parameters With Set or Add Commands</i>	<i>217</i>
<i>Table B.1: Specifications</i>	<i>226</i>
<i>Table B.2: Standards and Certifications</i>	<i>227</i>
<i>Table D.1: Device Type Differences.....</i>	<i>231</i>
<i>Table D.2: Reasons for Customizing Expect Scripts</i>	<i>232</i>
<i>Table D.3: Default Command Templates</i>	<i>235</i>
<i>Table D.4: Default Device Types and Corresponding Expect Scripts</i>	<i>242</i>
<i>Table D.5: Custom Device Types and Corresponding Expect Scripts</i>	<i>242</i>
<i>Table D.6: Expect Script Exit Codes</i>	<i>246</i>
<i>Table D.7: Tasks for Creating Addresses to Assign to Connected Devices</i>	<i>247</i>
<i>Table D.8: IP Address Ranges Reserved for Internal Network Addressing.....</i>	<i>248</i>
<i>Table D.9: Values for Configuring a Private Subnet</i>	<i>250</i>
<i>Table D.8: Examples for Creating IPSec and PPTP VPN Connections for Example 2.....</i>	<i>258</i>
<i>Table D.12: Information Defining a Virtual (DNAT) Network</i>	<i>264</i>
<i>Table E.2: Options for the create_cf command.....</i>	<i>279</i>

Installation Introduction

This chapter describes the available models, the private and public Ethernet ports, LEDs, power options and all other connectors on the Cyclades OnBoard service processor (SP) manager and provides additional prerequisite information needed for understanding the rest of the information in this guide.

The following list shows the topics covered in this chapter.

- *OnBoard Appliance Connectors* on page 1
- *OnBoard Appliance Models* on page 3
- *LEDs* on page 3
- *PCMCIA Card Slots* on page 5
- *Modem Types and Options* on page 5
- *Console Port* on page 6

OnBoard Appliance Connectors

The OnBoard appliance is a 1U SP manager that serves as a single access point for administering the following types of devices:

- Servers that have SPs with dedicated Ethernet ports
- Other devices that have dedicated Ethernet ports that provide console access

Figure 1.1 illustrates the front of an OnBoard appliance 1040 DAC (dual-AC power supply) model with two PCMCIA card slots and with two AC universal power inlets. Other models are available with one AC power supply or two DC power supplies, as described in *OnBoard Appliance Models* on page 3.

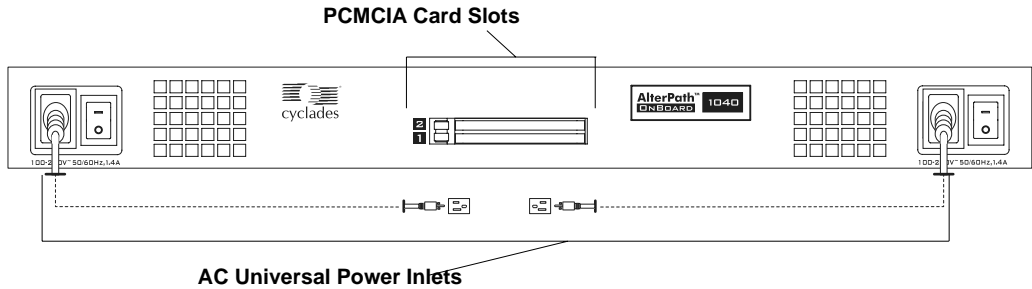


Figure 1.1: OnBoard Appliance Front With PCMCIA Card Slots and Two AC Power Inlets

DC models with two power supplies come with terminal blocks, as shown in the following figure.

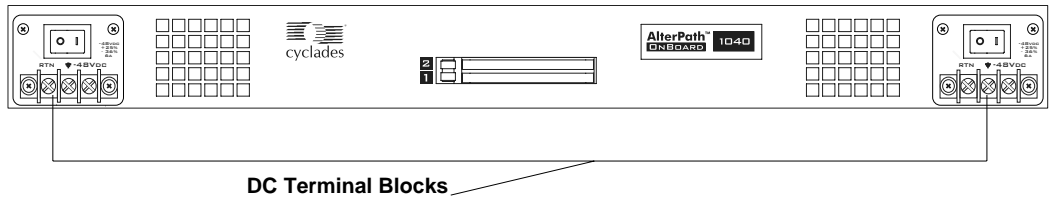


Figure 1.2: OnBoard Front With PCMCIA Card Slots and Two DC Terminal Blocks

Figure 1.3 illustrates the back of an OnBoard appliance model that has 40 private 10/100 Ethernet ports.

Figure 1.3 also illustrates the other ports that are standard on all OnBoard models: one public 10/100/GE (Gigabit Ethernet) primary Ethernet port, one public 10/100 secondary Ethernet port, one auxiliary (AUX) port and one console port.

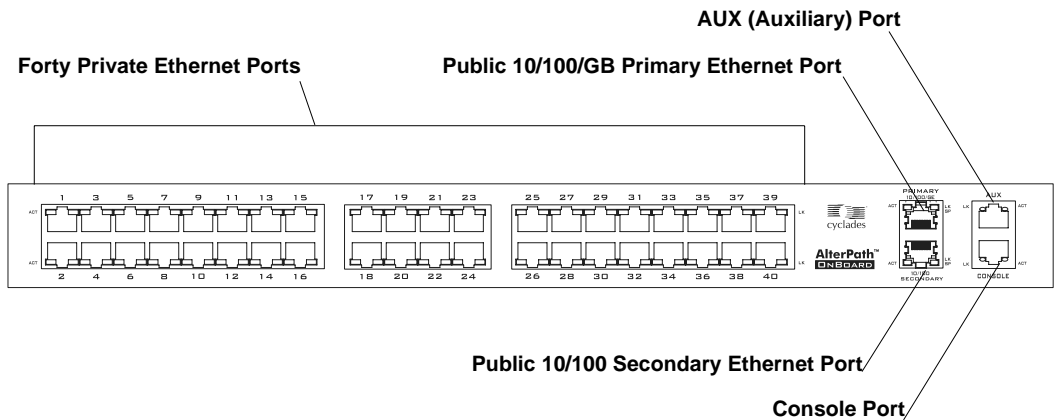


Figure 1.3: OnBoard Appliance Back With Ethernet, AUX, and Console Ports

After devices are connected to the OnBoard appliance, the administrator must configure the devices as described in Chapter 4.

OnBoard Appliance Models

The following table lists the number and types of power supplies and numbers of public Ethernet ports for each model.

Table 1.1: OnBoard Appliance Models

Model	Power Supply #	Power Type	# of Private Ethernet Ports
OnBoard1024 SAC	1	AC	24
OnBoard1040 SAC	1	AC	40
OnBoard1024 DAC	2	AC	24
OnBoard1040 DAC	2	AC	40
OnBoard1024 DDC	2	DC	24
OnBoard1040 DDC	2	DC	40

LEDs

Each private 10/100 Megabit/second Ethernet port has two LEDs. The following figure illustrates a close-up view of LEDs on some of the private Ethernet ports. The LED on the left blinks green for any detected activity (*ACT*). The LED on the right (*LK/SP*) is solid green when the speed is 100 Megabits/second and it is solid yellow when the speed is 10 Megabits/second.

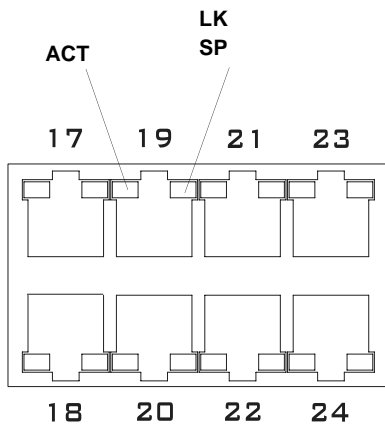


Figure 1.4: LEDs for Private Ethernet Ports

The following figure shows a close up view of the labels on the LEDs on the back right of the OnBoard appliance with numbered callouts. The LEDs in Figure 1.5 monitor the public Ethernet ports, the AUX port and the console port. The LEDs are described in Table 1.2.

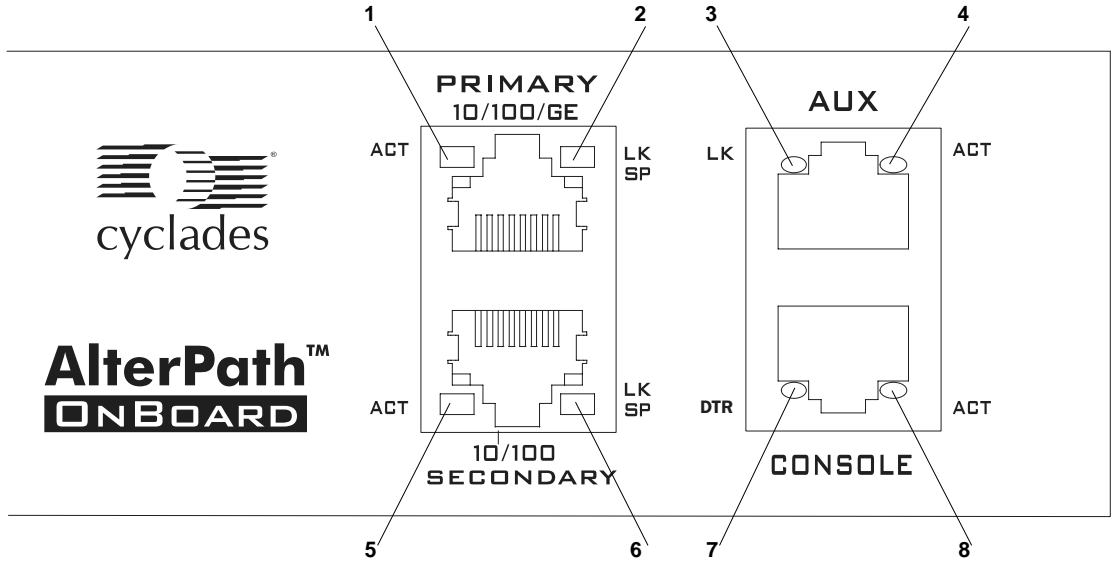


Figure 1.5: LEDs for AUX, Public Ethernet and Console Ports (Back).

Table 1.2: LED Descriptions

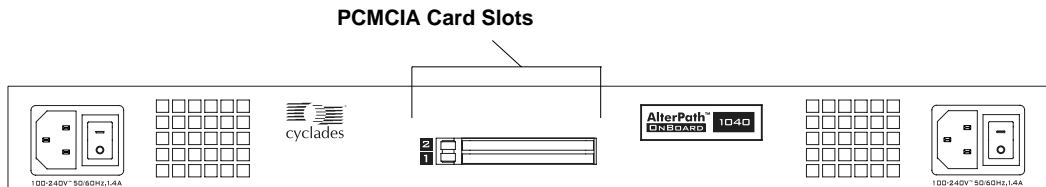
Number	Label	Function	Color/Status
1,5, and the left LED on all private Ethernet ports	ACT	Monitor Ethernet activity	<ul style="list-style-type: none"> • OFF – Indicates no activity. • Green – Blinks for any activity.
2,6, and the right LED on all private Ethernet ports	LK/SP	Monitor Ethernet link and speed	<ul style="list-style-type: none"> • OFF – Indicates either link is not up or cable is not connected. • Green – Indicates the speed is 100 or 1000 Megabits/second. • Yellow – Indicates the speed is 10 Megabits/second.
3	LK	Monitor RS-232 link	<ul style="list-style-type: none"> • OFF – Indicates either link is not up or cable is not connected. • Green – Lights solid when the link is up and blinks when activity occurs, with frequency proportional to traffic.

Table 1.2: LED Descriptions (Continued)

Number	Label	Function	Color/Status
4,8	ACT	Monitor RS-232 async activity	<ul style="list-style-type: none"> • OFF – Indicates no data activity. • Green – Blinks when data is either being received (RX) or transmitted (TX).
7	DTR	Monitors console port for transmissions	<ul style="list-style-type: none"> • OFF – Indicates OnBoard appliance is not ready to communicate. • ON – Indicates OnBoard appliance is ready to communicate.

PCMCIA Card Slots

Two PCMCIA type 2 card slots on the front of the OnBoard appliance, as shown in the following figure, offer additional remote access and storage options.

**Figure 1.6: PCMCIA Slots on the OnBoard Appliance Front**

Go to <http://www.cyclades.com> and select *Products-Cyclades OnBoard Service Processor Manager* to see a list of supported PCMCIA cards.

After inserting the PCMCIA card into the OnBoard appliance, the administrator must configure the card as described in Chapter 9.

Modem Types and Options

Modems can be connected to the OnBoard appliance in one of the two following ways:

- An external modem can be connected to the AUX port on the back
- A PCMCIA modem card can be inserted into a PCMCIA slot on the front

Cyclades Power Management (PM) Intelligent Power Distribution Units (IPDUs) can be connected to the AUX port on the OnBoard appliance. Any combination of models of Cyclades PM IPDUs can be daisy-chained to support management of up to a maximum of 128 outlets.

After an IPDU is connected to the OnBoard appliance, AC-powered devices of any type can be plugged into the IPDU. Authorized users can remotely manage power for the connected devices after the administrator does the following tasks:

- Configures the AUX port for power management
- Configures the outlets on connected IPDUs by specifying names to identify devices that are plugged into the outlets and by authorizing users to power devices connected to outlets up and down

The administrator may also configure notifications of over-current states to be sent as alarms to specified users.

Console Port

The console port is an RS-232 port used for connecting either a terminal or a computer running a terminal emulation program to enable local administration to use the command line. Local OnBoard appliance users can access the command line by logging in through this console port.

CHAPTER

2

Basic Installation Procedures

Figure 2.1 illustrates one possible configuration for your OnBoard appliance.

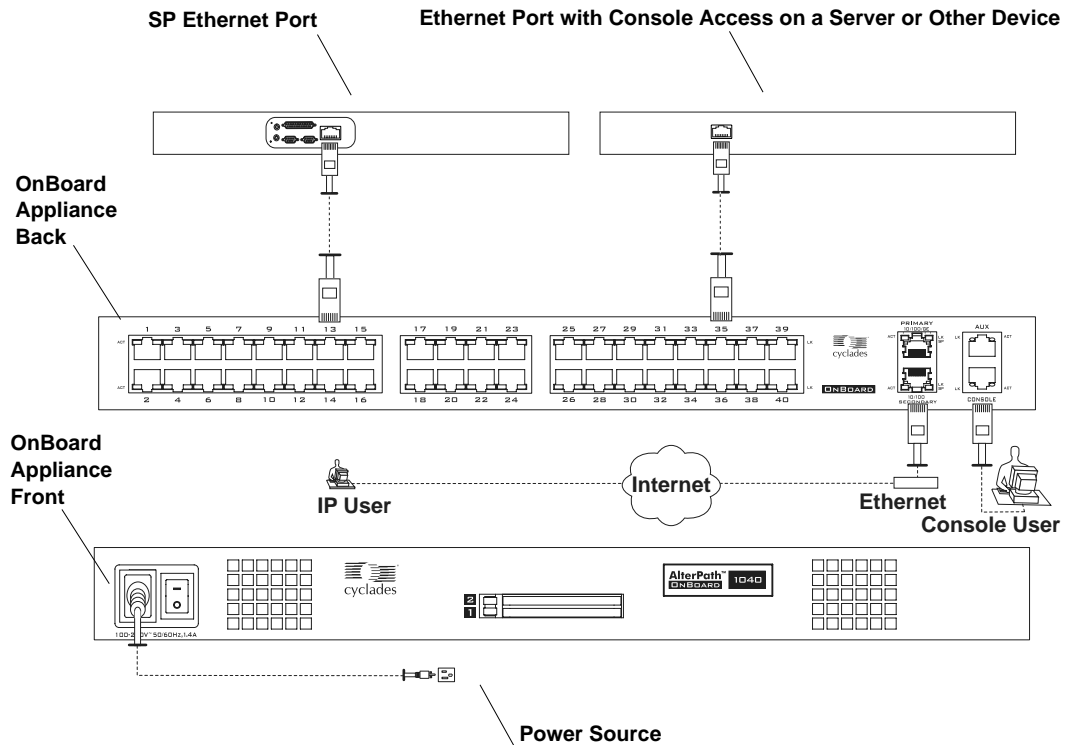


Figure 2.1: Basic Installation Connections Illustrated

Getting Started

Table 2.1 lists the basic tasks for installing the Cyclades OnBoard Service Processor Manager and the sections where the tasks are described in more detail.

CAUTION: Before you start installation, make sure you review and follow the safety precautions listed in *Safety Information* on page 228.

Table 2.1: Tasks for Basic Installation

Task	Where Documented
Review the contents of the shipping box.	<i>Supplied with the OnBoard Appliance</i> on page 9
Rack mount the OnBoard appliance.	<i>Rack Mounting the Cyclades OnBoard SP Manager</i> on page 9
Connect the public network to one or both of the public Ethernet ports.	<i>Making Public Ethernet Connections</i> on page 10
Connect SPs and other supported devices to the private Ethernet ports.	<i>Connecting Devices</i> on page 11
Connect the OnBoard appliance to a power source and power it up	<i>Connecting to a Power Source and Powering Up</i> on page 11
Chose a method to enable access to the Web Manager for completing user and device configuration and do one of the following sets of tasks:	<i>Methods for Enabling Web Manager Access</i> on page 13
To use a connection to the OnBoard appliance's console to set a static IP address, connect a terminal to the console port, collect needed network information and set the basic network parameters.	<ul style="list-style-type: none"> • <i>Connecting a Terminal to Configure Basic Network Parameters</i> on page 14 • <i>To connect a terminal to the console port:</i> on page 14 • <i>To configure basic network parameters using a terminal:</i> on page 15
If using DHCP, discover and use the DHCP-assigned IP address.	<ul style="list-style-type: none"> • <i>To use a dynamic IP address to access the Web Manager:</i> on page 16
If using the default IP address assigned to the OnBoard appliance, reconfigure the network portion of the IP address of a computer on the same network, so you can access the Web Manager and set a static IP address.	<ul style="list-style-type: none"> • <i>To use the default IP address to access the Web Manager:</i> on page 16
Select a security profile, add users and configure security and services using the Web Manager.	<i>Selecting a Security Profile, Adding Users and Configuring Devices Using the Web Manager</i> on page 17

For how to perform optional advanced procedures [connecting PCMCIA cards, Cyclades PM

intelligent power management modules (IPDUs) and external modems], see Chapter 3.

Supplied with the OnBoard Appliance

Before installing your OnBoard appliance, refer to the following list to ensure you have all items that come with the appliance.

- Cyclades OnBoard Service Processor Manager Quick Installation Guide
- Rack mounting brackets (2) and screws (8)
- For AC models, an AC power cable.
- RJ-45 to RJ-45 7ft CAT 5 cable
- DB-9 female to RJ-45 6 ft crossover cable

Rack Mounting the Cyclades OnBoard SP Manager

You can rack mount the OnBoard appliance in a rack or cabinet, mounting it either at the front or the back. Observe all safety precautions described in *Safety Information* on page 228, especially making sure to load the rack from the bottom up.

Before you start, make sure you have the following:

- The two brackets and the eight Phillips screws that are shipped with the OnBoard appliance
- A Phillips screwdriver
- Appropriate nuts and bolts for attaching the OnBoard appliance brackets to the rack

Decide whether to mount the OnBoard appliance on the front or back and locate the appropriate sets of holes on the OnBoard appliance. The locations of the holes for front and back mounting are shown in the following figure.

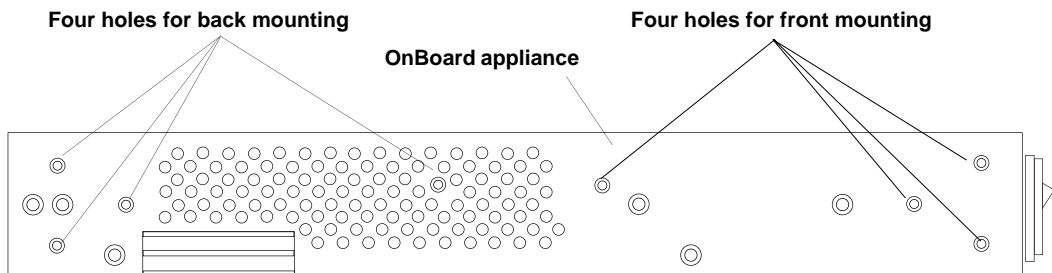


Figure 2.2: Bracket Mounting Holes on the OnBoard appliance's Right Side

To rack mount the OnBoard appliance:

1. Attach the right bracket to the right side and the left bracket to the left side of the OnBoard appliance.
 - a. For each bracket, insert four screws through the holes on the bracket into the appropriate holes at either the front or back of the OnBoard appliance.

- b. Use a Phillips screwdriver to tighten the screws.
2. Use the appropriate mounting hardware to mount the OnBoard appliance to the rails.

Making Public Ethernet Connections

The two Ethernet ports found on the right side of the back of the OnBoard appliance are for public connections.

The primary Ethernet port must be connected to an Ethernet switch, router or local area network (LAN) that provides Internet access, to enable remote configuration of the OnBoard appliance and remote access to connected devices.

The secondary Ethernet port can be optionally used in the following ways:

- To connect to a second network
- To connect to the same network as the primary Ethernet port for redundancy in case of failure of the primary port (referred to as Ethernet failover or bonding)

With a failover configuration, the OnBoard appliance administrator needs to enable failover. The tasks are described in *For more information, see the following sections.* on page 42.

With failover enabled, if the first Ethernet port fails, the second one automatically becomes active until the first one recovers.

One or more optional Ethernet PCMCIA cards may be inserted and configured to support the following:

- A second, third or fourth network (depending on how the two public Ethernet ports are configured)
- If failover is configured, a second, third or fourth failover interface

You can use the RJ-45 to RJ-45 Ethernet CAT 5 cable shipped with the OnBoard appliance or an off-the-shelf CAT 5 or greater cable (such as CAT 5e) to connect the Ethernet ports to Ethernet switches, routers or local area network (LAN) ports.

To make a public Ethernet connection:

1. Connect one end of a standard Ethernet cable to an Ethernet switch, router or LAN port.
2. If you are making one Ethernet connection, connect the other end of the cable to the primary Ethernet port on the OnBoard appliance.
3. If you are setting up Ethernet failover, connect a second cable from the same network to the secondary Ethernet port.
4. If you are using an optional Ethernet PCMCIA card on the OnBoard appliance, connect a cable between one of the Ethernet connections listed in step 1 to the PCMCIA card.

Connecting Devices

The 24 or 40 Ethernet ports found on the left side of the back of the OnBoard appliance are for private connections to SPs or to devices such as some servers and routers that provide console access or another type of management access through a dedicated Ethernet port.

CAUTION: To comply with FCC and CE certification requirements, use shielded cables when connecting devices to the Ethernet ports.

To prepare to connect devices to the OnBoard appliance:

1. Make sure all configuration is complete on devices to be connected.
2. For the device to use remote authentication, make sure that the following prerequisite configuration is complete:
 - Authentication servers are installed and fully configured
 - You have obtained from each authentication server's administrator the information (such as the IP address and other authentication-method specific information), which is needed to configure the authentication server on the OnBoard appliance.

NOTE: After the OnBoard appliance is installed, make sure to configure the desired authentication method for each device.

To connect devices to the private Ethernet ports:

Connect a standard Ethernet cable from the private Ethernet ports on the OnBoard appliance to any of the following types of Ethernet ports on the other end:

- A dedicated Ethernet port on an SP
- A dedicated Ethernet port on a router or other device that gives access to the device's console
- A switch that is connected to multiple devices (not recommended)
- A dedicated Ethernet port on a blade managing multiple SPs

Connecting to a Power Source and Powering Up

The OnBoard appliance comes with either one or two power supplies. When the OnBoard appliance has two power supplies, connect each power supply to a separate power source for redundancy in case one power source fails. The power sources must be independent of each other and must be controlled by separate circuit breakers.

To connect AC power inlets to an AC power source and power up:

1. Make sure the OnBoard appliance's power switch(es) are off.
2. Plug the power cord(s) into the OnBoard appliance and plug the other end(s) into an appropriate grounded power source(s).

NOTE: On dual AC models, plug the power cords into separate power sources.

3. Power up the OnBoard appliance.

To connect DC power terminal blocks to a DC power source and power up:

1. Make sure the OnBoard appliance's power switch(es) are off.
2. Do the following steps twice to wire both terminal blocks to independent power sources.
 - a. Loosen the hex screw labeled RTN, attach the red wire (positive) from the DC power supply to the screw and tighten the screw again.
 - b. Loosen the hex screw labeled -48VDC, attach the black wire (return) from the DC power supply to the screw and tighten the screw again.

Figure 2.3 illustrates the red wire connected between the positive connector and the RTN screw and the black wire connected between the negative connector and the -48VDC screw.

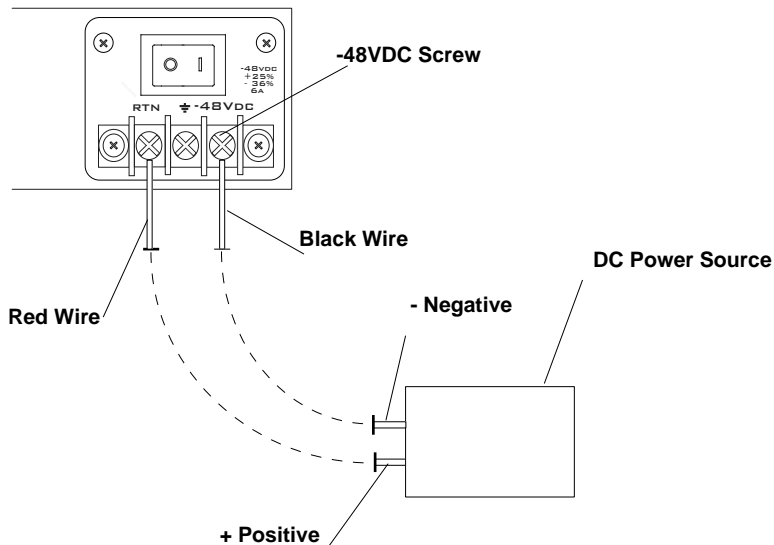


Figure 2.3: Wiring the DC Power Terminal to Positive and Negative DC Power Connectors

- c. Loosen the hex screw labeled with the ground symbol, attach a green grounded wire to the screw and tighten the screw again.

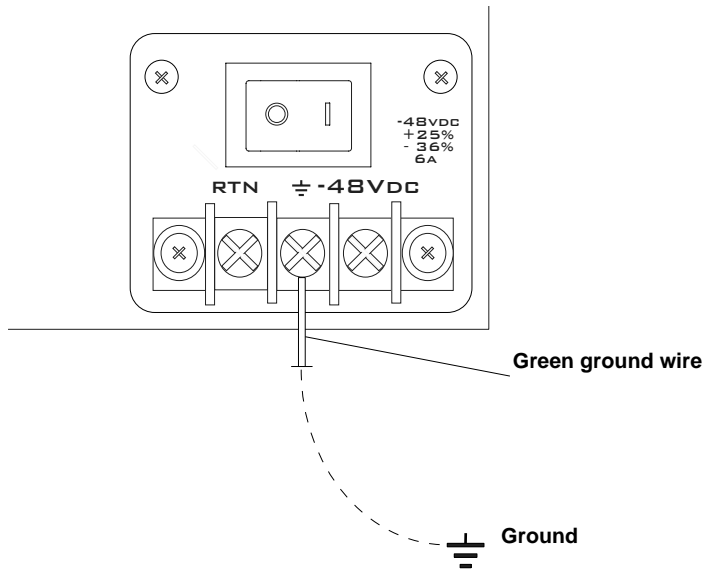


Figure 2.4: Wiring the DC Power Terminal to Ground

3. Power up the OnBoard appliance.

Methods for Enabling Web Manager Access

An administrator who knows the password for an administrative user account and who has network access to the OnBoard appliance needs to enter the OnBoard appliance's DNS name or IP address in a browser to bring up the Web Manager and to finish the configuration of users and connected devices.

Perform one of the tasks in the following table to set a static IP address or set up a DHCP server, so that the basic network configuration can be done to enable the administrative user to use the Web Manager to finish configuration.

Table 2.2: Methods for Enabling Web Manager Access

Method	Considerations	Where Described
Connect a terminal to the console port and use the <code>cycli</code> command to assign a static IP address.	You must be at the same location as the OnBoard appliance to make the local connection.	<i>Connecting a Terminal to Configure Basic Network Parameters</i> on page 14
Use the DHCP-assigned address.	DHCP is enabled by default. It relies on a DHCP server that must be available to the OnBoard appliance.	<i>To use a dynamic IP address to access the Web Manager:</i> on page 16

Table 2.2: Methods for Enabling Web Manager Access (Continued)

Method	Considerations	Where Described
Use the default OnBoard appliance IP address 192.168.160.10 to bring up a Web Manager to set a fixed IP address.	You must temporarily change the network portion of the IP address of a computer on the same subnetwork as the OnBoard to be able to use the default IP address in launching the Web Manager.	<i>To use a dynamic IP address to access the Web Manager:</i> on page 16

Connecting a Terminal to Configure Basic Network Parameters

If you connect a terminal or workstation to the console port, you can use the `cycli` utility to configure basic network parameters as described in *To configure basic network parameters using a terminal:* on page 15. An RJ-45 to DB-9 6 ft crossover cable is shipped with the OnBoard appliance for the connection.

Perform the following steps to connect a terminal or a workstation to the console port of the OnBoard appliance. If connecting a PC, ensure that HyperTerminal or another terminal emulation program is installed on the Windows operating system. On a workstation running a UNIX-based operating system, such as Linux or Solaris, make sure that a compatible terminal emulator such as Kermit or Minicom is installed.

This procedure assumes you have the RJ-45 to DB-9 6 ft CAT 5 cable shipped with the OnBoard appliance or an off-the-shelf equivalent CAT 5 or greater cable. If the terminal or workstation has a USB port, you also need a USB to DB-9 converter.

NOTE: Be sure that whatever cable you use is a crossover cable.

To connect a terminal to the console port:

1. If connecting to a workstation or terminal with a DB-9 male port, perform these steps.
 - a. Connect the RJ-45 end of the cable to the OnBoard appliance's console port.
 - b. Connect the DB-9 male end of the cable to the DB-9 connection on the terminal or workstation.
2. If connecting to a workstation or terminal with a USB port, perform these steps.
 - a. Connect the RJ-45 end of the cable to the OnBoard appliance's console port.
 - b. Connect the DB-9 female end to the DB-9 male end of a USB converter.
 - c. Connect the USB end of the converter to a terminal or workstation.

Enabling Access to the Web Manager

Perform the procedures in this section to enable a remote administrator to finish configuration using the Web Manager. These procedures requires a terminal or a computer that has a terminal emulation program to be physically connected to the console port of the OnBoard appliance.

To configure basic network parameters using a terminal:

1. Using either a terminal or a terminal emulation program installed on a computer that is connected to the OnBoard appliance, start a session with the following console port settings:

Serial Speed: 9600 bps

Parity: None

Flow Control: None

Data Length: 8 bits

Stop Bits: 1

ANSI emulation

2. Log into the console port as the root user with the default password cyclades.

CAUTION: It is recommended that the default password for the root user be changed immediately.

3. Enter the **passwd** command, and enter and confirm a new password when prompted.

```
[root@OnBoard /]# passwd
```

4. Invoke the **cycli** utility.

```
[root@OnBoard /]# cycli
```

5. Make sure the primary Ethernet interface (eth0) is active.

```
cli> set network interface eth0 active yes
```

NOTE: Alternately, you can enter all the set network interface eth0 parameters in step 5 through step 10 in a single cycli command line.

6. Specify static as the method (to set a static IP address).

```
cli> set network interface eth0 method static
```

7. Specify an IP address for the OnBoard appliance.

```
cli> set network interface eth0 address onboard_IP_address
```

8. Specify a gateway IP address.

```
cli> set network interface eth0 gateway gateway_IP_address
```

9. Specify the netmask.

```
cli> set network interface eth0 netmask netmask
```

10. Specify the broadcast address for the OnBoard appliance.

```
cli> set network interface eth0 broadcast broadcast_IP_address
```

11. Specify the hostname for the OnBoard appliance.

```
cli> set network hostname OnBoard_name
```

12. Specify the domain name.

```
cli> set network resolv domain domain_name
```

13. Enter the IP address for the primary DNS (domain name) server.

```
cli> set network resolv dns0 DNS_server_IP_address
```

14. Optional, enter the IP address for a secondary DNS (domain name) server.

```
cli> set network resolv dns1 secondary_DNS_server_IP_address
```

15. Confirm the configuration for the interface.

```
cli> get network interface eth0
```

16. Confirm the name server configuration.

```
cli> get network resolv
```

17. Save the changes.

```
cli> commit
```

18. Exit from the cycli utility.

```
cli> quit
```

19. Log out and enter the IP address in a browser to bring up the Web Manager to add users and configure access to devices as desired.

20. Finish configuring security, users and devices the OnBoard appliance using the Web Manager.

To use a dynamic IP address to access the Web Manager:

This procedure assumes that DHCP is enabled and that you know the IP address that is currently assigned to the OnBoard appliance from a DHCP server on the same subnet.

1. Use the OnBoard appliance's dynamically-assigned IP address in a browser to bring up the Web Manager.
2. Finish configuring users and the OnBoard appliance parameters using the Web Manager.
3. Make sure that the root user changes the password by logging into the OnBoard appliance console. See *To change root's password:* on page 17.

To use the default IP address to access the Web Manager:

NOTE: The default IP address for the OnBoard appliance is 192.168.160.10. This procedure assumes that you are able to temporarily change the IP address of a workstation that is on the same subnet as the OnBoard appliance.

1. On a workstation that has a physical network connection to the OnBoard appliance, change the network portion of the IP address of that workstation to 192.168.160 and make sure that the host portion of the IP address is not the same as the OnBoard appliance.
2. Bring up a browser on the workstation whose address you changed, enter the OnBoard appliance's default IP address (<http://192.168.160.10>) to bring up the Web Manager, and log in.

3. To allow subsequent use of the Web Manager from any workstation, go to the Wizard-Network Settings option to change the OnBoard appliance's IP address to a fixed public IP address and to configure the other basic network parameters.
4. Restore the workstation's IP address to its previous IP address.
5. Make sure that the root user changes the root password by logging into the OnBoard appliance console.

Changing the root User's Password

Whatever method is used to enable access to the Web Manager, the root user must always log into the OnBoard appliance console and change the password from the default, which is `cyclades`. The admin user cannot change the root user's password, and the root user cannot log into the Web Manager to change the password. The following options are available:

- Until an IP address is available for the OnBoard appliance, the only way that root can change the root password is to log in locally through the console port. See *To configure basic network parameters using a terminal*: on page 15.
- After an IP address is available for the OnBoard appliance, the remote root user can use `ssh` to connect to the OnBoard appliance console and log in from a remote location and change the password.

To change root's password:

1. Use SSH to connect to the console using the OnBoard appliance's IP address or DNS name.
2. When prompted, login as root.

```
OnBoard login: root
Password: cyclades
[root@OnBoard /root]#
```

The default password is `cyclades`.

3. Enter the `passwd` command, and enter and confirm a new password when prompted.

```
[root@OnBoard /root]# passwd
```

Selecting a Security Profile, Adding Users and Configuring Devices Using the Web Manager

For the configuration tasks the administrator needs to perform, see Chapter 4. These tasks include selecting a security profile, adding users and configuring devices.

For how OnBoard appliance administrators and regular users access the OnBoard appliance and perform device management actions on connected devices, see the *Cyclades OnBoard Service Processor Manager User Guide*.

Advanced Installation Topics and Tasks

Installing PCMCIA Cards in the Front Card Slots

Two PCMCIA cards of different types can be installed in any order. Two PCMCIA cards of the same type, however, must be installed with the card in slot 1 configured first, followed by the card in slot 2.

Swapping in a new PCMCIA card may result in the configuration being lost on one or both of the cards. Follow the procedure under *To swap in a new PCMCIA card:* on page 20 to remove any existing cards, then insert and configure the new card and reinsert and reconfigure the old card.

To install a PCMCIA card:

NOTE: Some cards take up both card slots.

1. Insert a PCMCIA card into a front slot(s) and slide the card in until it is firmly seated.
2. If installing a modem card, use a phone cord to connect the card to a live telephone line.
3. Use the Web Manager-Settings-PCMCIA form to configure the PCMCIA card.
 - a. Click the *Insert* button on the form next to the number of the slot where the card is installed. A prompt displays asking if you have inserted the card into the slot.
 - b. Click *Yes*.
 - c. Click the *Configure* button. A PCMCIA card configuration form appears.
 - d. Select a card type from the Card Type pull-down menu. Fill out the fields and select among the choices on the menus.

To remove a PCMCIA card:

1. On the Web Manager-Settings-PCMCIA form, select the *Eject* button next to the card's slot number.
2. On the front of the OnBoard appliance, press the button next to the PCMCIA slot.
3. Remove the card from the slot.

To swap in a new PCMCIA card:

Complete the following steps if only one card slot is in use, you wish to replace the current card (or add a new one) and the new card is the same as the one already installed.

1. Eject the card.
2. If only one slot is currently in use, insert and configure the new card.

-or-

If both slots are in use, press the buttons next to both PCMCIA slots on the front of the OnBoard appliance. Then insert and configure the new card.

Connecting an External Modem to the AUX Port

An external modem can be connected to the AUX port on the back of the appliance.

Figure 3.1 illustrates connecting an external modem to an AUX port and connecting the modem to the telephone network.

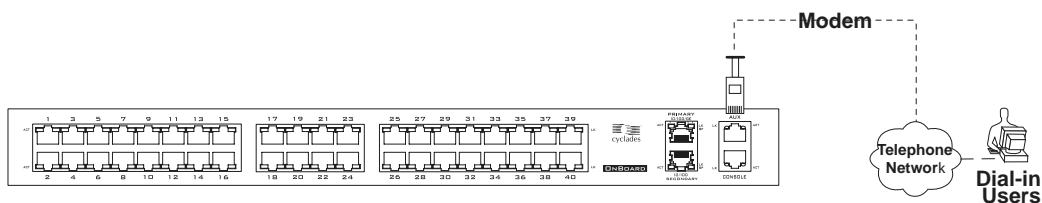


Figure 3.1: Connecting an External Modem to the AUX Port and to the Telephone Network

This procedure requires the following cables and connectors:

- A straight-through CAT 5 or greater cable for connecting the AUX port to the external modem, with a RJ-45 connector on one end and the appropriate connector or adaptor (USB, DB-9 or DB-25) on the other end.
- A phone cord (for connecting the modem to a live phone line) with RJ-11 connectors on both ends.

To connect an external modem to the AUX port:

1. Connect the RJ-45 end of the cable to the AUX port on the OnBoard appliance.
2. Connect the other end of the cable to the modem.
3. Connect the phone cord between the jack on the modem and a live telephone jack at your site.
4. Configure the AUX port for PPP.

See *Configuring the AUX port for a modem* on page 115 for details.

Connecting One or More IPDUs to the AUX Port

You can daisy-chain any combination of Cyclades PM IPDUs to the AUX port with up to a total of 128 outlets. You need a straight-through RJ-45 to RJ-45 CAT 5 or greater cable for connecting the IPDU to the OnBoard appliance, and you need another straight-through RJ-45 to RJ-45 CAT 5 or greater cable for each IPDU to be daisy-chained.

NOTE: Do not plug the OnBoard appliance into an IPDU that is connected to the OnBoard appliance's AUX port.

To connect an IPDU to the AUX port:

1. Connect one end of the cable to the AUX port on the OnBoard appliance.
2. Connect the other end of the cable to the In port of the IPDU.
3. Configure the AUX port for Power Management. See *Configuring the AUX port for IPDU power management* on page 115 for details about configuring the AUX port.

To daisy-chain multiple IPDUs to the OnBoard appliance:

1. Connect one end of the cable to the Out port of an IPDU that is already connected to the AUX port of a OnBoard appliance.
2. Connect the other end of the cable to the In port of the next IPDU.
3. Repeat steps 1 and 2 until you have connected the desired number of IPDUs.
4. Configure the AUX port for power management.

See *Configuring the AUX port* on page 115.

NOTE: Make sure that all daisy-chained IPDUs are running the same firmware version./

Introduction for Administrative Users

The administrator configures the OnBoard appliance to enable controlled access to connected devices and also performs maintenance activities such as upgrading the OnBoard appliance firmware.

Overview of OnBoard Appliance Features for Administrators

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

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

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

The OnBoard appliance provides a set of security features not available in any SP management product from any other vendor. The following table lists the features that OnBoard appliance 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 4.1: Security Features and Where Documented

Security Feature	Where Documented
Authentication for accessing the OnBoard appliance and connected devices	<i>OnBoard Appliance Authentication Options</i> on page 24
One-time passwords	<i>One-time Password Authentication on the OnBoard Appliance</i> on page 28
Authorizations assigned to users and groups to control access to connected devices	Cyclades OnBoard Service Processor Manager User Guide

Table 4.1: Security Features and Where Documented (Continued)

Security Feature	Where Documented
Security profiles and other means for controlling which network services are turned on or blocked and for setting other security parameters	<ul style="list-style-type: none"> • <i>OnBoard Appliance Security Profiles</i> on page 30 • <i>OnBoard Appliance Services</i> on page 32
<i>Logging, notifications and alarms</i> that can alert remote administrators about problems and <i>data buffering</i> to capture and monitor user activity.	<ul style="list-style-type: none"> • <i>OnBoard Appliance Notifications</i> on page 45 • <i>Configuring Notifications</i> on page 152 • <i>OnBoard Appliance Sensor Alarms</i> on page 46 • <i>Configuring Sensor Alarms</i> on page 155 • <i>SNMP on the OnBoard Appliance</i> on page 35 • <i>Configuring SNMP</i> on page 161 • <i>Data Buffering on the OnBoard Appliance</i> on page 52 • <i>Firewall/Packet Filtering on the OnBoard Appliance</i> on page 53

OnBoard Appliance Authentication Options

The OnBoard appliance administrator can configure many common authentication methods for logins to the OnBoard appliance or to connected devices. By default, all logins to the OnBoard appliance and connected devices use Local authentication.

See the authentication-related considerations in the following bulleted list. These authentication methods use both local authentication and authentication servers in the order shown: Local/AuthType, AuthType/Local and then AuthType/DownLocal.

- The AuthType/Local and AuthType/DownLocal authorization methods are referred to as authentication methods with local fallback options
- Administrators can specify separate authentication types for OnBoard appliance logins and for connected devices
- Local and OTP authentication methods and the authentication methods that have local fallback options require user accounts configured on the OnBoard appliance

If configuring any authentication method other than Local, the administrator user must make sure an authentication server is set up for that method as itemized in the following list.

- The OnBoard appliance must have network access to an authentication server set up for every authentication method specified.
- Each authentication server must be configured and operational.
- The administrator configuring the OnBoard appliance 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 appliance.

NOTE: This section discusses only the types of authentication used for controlling who can access the OnBoard appliance 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 appliance and which are available for connected devices. When a table cell is blank, the authentication method is not supported.

Table 4.2: Supported Authentication Types

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

Table 4.2: Supported Authentication Types (Continued)

Type	Description	OnBoard Appliance	Device
Local/NIS	Uses NIS authentication if local authentication fails.	X	X
OTP	Uses the one-time password (OTP) authentication method.		X
OTP/Local	Uses the local password if the OTP password fails.		X
RADIUS	Uses user/password configured on the RADIUS authentication server. No logins allowed if NIS server is down or NIS authentication fails.	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 user/password configured on the SMB authentication server (for Microsoft Windows NT/2000/2003 Domain). No logins allowed if SMB server is down or SMB authentication fails.	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 user/password configured on the Terminal Access Controller Access Control System (TACACS+) authentication server. No logins allowed if NIS server is down or NIS authentication fails.	X	X
TACACS+ Down/Local	Uses local authentication if TACACS+ server is down.	X	X
TACACS+/Local	Uses local authentication if TACACS+ authentication fails.	X	X
Local/TACACS+	Uses TACACS+ authentication if local authentication fails.	X	X

An administrative user can use the Web Manager, and any administrator can use the cycli utility for configuring an authentication method for the OnBoard appliance and 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 4.3: Tasks for Configuring Authentication

Task	Where Documented
Decide which authentication methods are going to be used for logins to the OnBoard appliance and for logins to connected devices.	Table 4.2 on page 25
Make sure an authentication server for each method is accessible to the OnBoard appliance and work with the server(s)' administrators to obtain the information needed to configure the servers on the OnBoard appliance and to make sure the required accounts are set up on the servers.	N/A
On the OnBoard appliance, configure an authentication server for each authentication method.	<i>Configuring authentication servers</i> on page 144
Specify the OnBoard appliance login authentication method or accept the default Local authentication method.	<i>Configuring an authentication method for the OnBoard appliance</i> on page 151
(Optional:) Create a custom security profile that specifies authentication method to be assigned to all subsequently-created devices. (The specified authentication method can be overridden during configuration of new devices.)	<i>Selecting or Configuring a Security Profile</i> on page 169
While creating new devices, assign the desired authentication method to each device.	<i>Configuring devices</i> on page 106
Give users the username and password information they need for being authenticated on the devices.	N/A
Configure either an external modem connected to an AUX port, or a modem or GSM or CDMA phone PCMCIA card for dial-in logins with OTP authentication and give users the OTP information they need to be authenticated for dial-ins.	<i>One-time Password Authentication on the OnBoard Appliance</i> on page 28

One-time Password Authentication on the OnBoard Appliance

OPIE (one-time passwords in everything) software (www.inner.netpub/opie) on the OnBoard appliance supports the OTP authentication method for certain types of access. This section describes the options the administrator has for configuring OTP authentication.

The OnBoard appliance root user must do the initial configuration manually (not through the Web Manager). The following table lists the configuration tasks and where they are documented.

Table 4.4: Tasks for Configuring OTP Authentication for Dial-ins

Task	Where Documented
Manually configure and mount a directory from an external storage device to use for storage of the OTP databases.	<ul style="list-style-type: none"> • <i>Specifying the Location for the OTP Databases</i> on page 60 • <i>To configure a PC compact Flash card for OTP database storage:</i> on page 60 • <i>To configure a NFS-mounted directory for OTP database storage:</i> on page 61
Configure OTP for various types of access, as desired.	<p>The following procedures that use the Web Manager provide a step for configuring OTP authentication for dial-ins:</p> <ul style="list-style-type: none"> • <i>To configure an AUX port for modem access:</i> on page 118 • <i>To configure a modem or GSM PCMCIA card:</i> on page 127 <p>The following procedures must be done manually.</p> <ul style="list-style-type: none"> • <i>To configure OTP authentication for SSH or console logins:</i> on page 61 • <i>To configure OTP authentication for a device:</i> on page 62
<p>Make sure each user who needs to use OTP has a local user account, is registered with the OTP system and is able to obtain the OTP username, OTP secret pass phrase and OTP passwords needed for logins. See the following list for options:</p> <ul style="list-style-type: none"> • Register each user yourself and give the OTP username and OTP secret pass phrase to each user. <p>-and-</p> <ul style="list-style-type: none"> • Generate the needed OTP passwords on behalf of the each user and give them to each user. <p>-or-</p> <ul style="list-style-type: none"> • Make sure users are equipped with an OTP generator that is not on the network to generate their own OTP passwords when challenged at login time. 	<ul style="list-style-type: none"> • <i>How Users are Registered with OTP and Obtain OTP Passwords</i> on page 62 • <i>To register and generate OTP passwords for users:</i> on page 63 • <i>Obtaining and Using One-time Passwords for Dial-ins in the Cyclades OnBoard Service Processor Manager User Guide.</i>

OnBoard User and Group Configuration Options

On the OnBoard appliance, a normal UNIX and an OnBoard appliance user account (called an onboard user) are needed to give a user access to the OnBoard appliance and to authorize the user for access to device management functions on connected devices.

Both types of user accounts are created transparently when an administrator adds a user through the Web Manager. When an administrator adds a new user through the cycli utility, the administrator needs to take separate steps to add the user as a regular and onboard user.

Configuring user and group accounts

The OnBoard appliance administrator configures user accounts by assigning parameters that are described in the following table.

Table 4.5: User Configuration Settings

Settings	Notes
Username	Login name required for the user account.
Full name	Administratively-defined name to identify the user (the UNIX GECOS).
Password	Password used for accessing the OnBoard appliance.
<ul style="list-style-type: none"> • Sensors • Event log • Device Console • Power • Service Processor Console • Native IP 	<p>Allow the user to perform the selected device management actions on individual devices or all devices.</p> <p>See the Cyclades OnBoard Service Processor Manager User Guide.</p>
PPP/PPTP access <ul style="list-style-type: none"> • None • PPP (dialup only) • PPTP (VPN only) • PPP (dialup) and PPTP (VPN) 	<p>Allow the user to use PPP or PPTP or both for contacting the OnBoard appliance. Requires a password, which may be different from the one required to access the OnBoard appliance.</p>

The administrator can assign users to a group to make it possible to multiple users to perform management actions on one or more connected devices

Tasks for configuring users and groups

Table 4.6: User and Group Configuration Tasks

Task	Where Documented
<ul style="list-style-type: none"> Authorize the user to access the OnBoard appliance through the Web Manager or through <code>ssh</code> by creating a user account and assigning it a password Authorize the user to access the OnBoard appliance using PPP or PPTP by specifying either or both types of access (PPP and PPTP) and specifying a PPP username and password Authorize the user to perform administrative actions on the OnBoard appliance by assigning the user to the preconfigured admin group Authorize the user to perform management actions on one or more connected devices 	<ul style="list-style-type: none"> <i>Configuring regular users</i> on page 108 <i>To create and authorize a user for device management:</i> on page 108 <i>Configuring Users and Groups</i> on page 140 <i>To modify a user's account:</i> on page 141
Create user groups and authorize them for device management the user to an administratively-configured group.	<ul style="list-style-type: none"> <i>Configuring groups</i> on page 140 <i>To create and authorize user groups for device management:</i> on page 142
Authorize the user to manage power on IPDUs	<ul style="list-style-type: none"> <i>Configuring users to manage power outlets on a connected IPDU</i> on page 121 <i>To configure a user to manage power outlets on a connected IPDU:</i> on page 122
Modify the menu displayed for all users at console login	<ul style="list-style-type: none"> <i>Configuring the User's Console Login Menu</i> on page 78 <i>To modify the user shell menu:</i> on page 79
<p>If the OTP authentication method is configured for dial-in login access to modem or phone PCMCIA cards, do the following:</p> <ul style="list-style-type: none"> Register users who need to dial-in to one of the PCMCIA cards with the OTP system Make sure users can obtain the OTP usernames, OTP secret pass phrase and OTP passwords they need to dial-in 	<ul style="list-style-type: none"> <i>One-time Password Authentication on the OnBoard Appliance</i> on page 28 <i>How Users are Registered with OTP and Obtain OTP Passwords</i> on page 62 <i>To register and generate OTP passwords for users:</i> on page 63

OnBoard Appliance Security Profiles

Each OnBoard appliance has a security profile defined during initial configuration. The type of security profile selected by the OnBoard appliance 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 *OnBoard Appliance Services* on page 32.

Table 4.7 describes the services that are enabled and disabled in the preconfigured security profiles: moderate, secured and open.

Table 4.7: Default Security Profile Services/ Features

This feature:	Is enabled in this security profile:	Is disabled in this security profile
HTTP	Moderate, Open	Secured
HTTPS	Moderate, Secured, Open	
ICMP	Moderate, Open	Secured
IPSec	Moderate, Open	Secured
PPTP	Moderate, Open	Secured
RPC	Open	Moderate, Secured
SNMP v1	Open	Moderate, Secured
SNMP v2c	Open	Moderate, Secured
SNMP v3	Open	Moderate, Secured
SSH v1	Open	Moderate, Secured
SSH v2	Secured, Open	Moderate
Telnet to OnBoard	Open	Moderate, Secured
Default authentication type to access devices set to Local	Moderate, Secured, Open	

If the administrator chooses to configure a custom security profile, the administrator can select among all the options listed in Table 4.7. In addition, the administrator can allow root logins using SSH, redirect HTTP to HTTPS, assign an alternate port to SSH, HTTP or HTTPS or select a default authentication type. After the customized security profile goes into effect, if a default authentication type is specified in a custom security profile, whenever a new device is configured the specified authentication type is selected by default in the Web Manager. Also, the specified authentication type is assigned by default to any new device configured using the cycli utility. The administrative user is always able to change the authentication type for each individual device.

OnBoard Appliance Services

A network service is available on the OnBoard appliance if the security profile enables the service or if the administrator has enabled the service through the Web Manager, 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.

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 4.8: Services That Require Additional Configuration

Service	Where Documented
DHCP	<i>DHCP on the OnBoard Appliance</i> on page 34
HTTPS	<i>HTTPS on the OnBoard Appliance</i> on page 34 and <i>To replace the self-signed certificate with one from a certificate authority:</i> on page 66
IPSec	<i>VPN on the OnBoard Appliance</i> on page 39 and <i>IPSec VPN connections</i> on page 71
PPTP	<i>VPN on the OnBoard Appliance</i> on page 39, <i>Configuring Users and Groups</i> on page 140 and <i>PPTP VPN connections</i> on page 73
NTP	<i>Configuring system date and time</i> on page 132
SNMP	<i>SNMP on the OnBoard Appliance</i> on page 35
Syslog	<i>Firewall/Packet Filtering on the OnBoard Appliance</i> on page 53
Telnet	<i>Telnet on the OnBoard Appliance</i> on page 33

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

- FTPD
- HTTP
- ICMP
- INETD

- PMD
- RPC
- SSH

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

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

Telnet on the OnBoard Appliance

Telnet is not encrypted, so the OnBoard appliance controls its use to protect communications. By default, the Telnet service is disabled, while a Telnet client is used for proxied communications between users on the public network and devices on the private network side of the OnBoard appliance.

Telnet service configuration

The Telnet service is not supported by any of the default security profiles and `telnetd` is not active to prevent users from using Telnet clients from remote workstations either to connect to the OnBoard appliance or to connect through the appliance to devices. (Encrypted SSH clients may be used instead.) An administrator may choose to enable the Telnet service. Even if the Telnet service is enabled, the OnBoard appliance-specific device management commands cannot be passed as parameters to the `telnet` command but only to the `ssh` command.

Telnet client configuration

A Telnet client is used when proxying communications between users and most types of devices on the private network because all supported device types support Telnet connections while some do not support SSH. (The OnBoard appliance uses `ipmitool` commands for IPMI-type SPs.) If an SP must be on the public network, then the administrator should strongly consider configuring either an SSH client or `bidilink` to be used instead of the Telnet client, if either SSH or `bidilink` is supported by the SPs.

Telnet configuration tasks

The following table shows tasks that may be performed to change the default Telnet configuration with links to where the tasks are documented.

Table 4.9: Tasks for Changing the Default Telnet Configuration

Change to Default Telnet Configuration	Where Documented
Enable the <code>telnetd</code> service to allow Telnet clients to connect to the OnBoard appliance or to connected devices	<i>Selecting or Configuring a Security Profile</i> on page 169 <i>To configure services:</i> on page 169

Table 4.9: Tasks for Changing the Default Telnet Configuration

Change to Default Telnet Configuration	Where Documented
Configure SSH or bidilink as the method used to create connections to devices on behalf of authorized users	<i>Configuring SSH or Bidilink Instead of Telnet for Device Connections</i> on page 65.

HTTPS on the OnBoard Appliance

For HTTPS (secure HTTP based on SSL) to work, an SSL certificate must be present on the OnBoard appliance, so a self-signed certificate is automatically generated. To reduce the risks posed by weaknesses inherent in self-signed certificates, OnBoard appliance administrators are strongly advised to replace the automatically-generated self-signed certificate with an SSL certificate from an official certificate authority (CA). See *To replace the self-signed certificate with one from a certificate authority*: on page 66 for the procedure.

DHCP on the OnBoard Appliance

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

DHCP client

The OnBoard appliance's DHCP client is active, with DHCP enabled by default for the primary Ethernet port. With the default configuration, if the OnBoard appliance cannot find a DHCP server on the same subnet, it falls back to using the default IP address.

DHCP server

A DHCP server (dhcpd) is present but disabled on the OnBoard appliance by default. The OnBoard appliance 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 appliance to keep the same IP address even after the OnBoard appliance or the device is rebooted.
- 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 appliance administrator can assign an IP address to a client before the OnBoard appliance 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 appliance. For that reason, the OnBoard appliance 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 48
- *Address configuration for connected devices* on page 247

The OnBoard appliance administrator can enable the DHCP server and assign IP addresses to devices by logging into the OnBoard appliance command line as root and manually editing the `/etc/dhcpd.conf` file and performing other steps described under *Configuring the DHCP Server* on page 68. Before deciding whether to use the DHCP server to configure addresses for connected devices, the OnBoard appliance administrator should understand the available options for assigning IP addresses to connected devices, which are described in *Address configuration for connected devices* on page 247.

SNMP on the OnBoard Appliance

The administrator can activate Simple Network Management Protocol (SNMP) agent software that resides on the OnBoard appliance. The SNMP agent provides access to the OnBoard appliance by an SNMP management application, such as HP Openview, Novell NMS, IBM NetView or Sun Net Manager and provides proxied access to SNMP data from connected SPs that implement SNMP agents. The OnBoard appliance SNMP agent can be configured to send notifications (also known as traps) about significant events on the OnBoard appliance and on connected devices.

The OnBoard appliance administrator must configure the SNMP agent to use the version of SNMP supported by the management application, either SNMP v1, v2c and v3. The use of v3 is strongly encouraged wherever possible because it provides authentication and encryption of data that is lacking in v1 and v2c.

Access to information provided by the OnBoard appliance and its proxied connected devices is available in two ways:

- The recommended access method for agents which support only SNMP version 1 or 2c is through a VPN tunnel to the OnBoard appliance. The OnBoard appliance provides the authentication and encryption lacking in those protocol versions. The management application can then be used to for SNMP management of the device.

When versions 1 or 2c agents are used to obtain native management access to a device, no SNMP configuration is needed. Support is implemented entirely through the VPN connection limited by iptables rules that restrict access to particular devices.

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 access method agent which supports version 3 is via a local Net-SNMP `snmp` daemon. The proxying of traps is not supported by `Net_SNMP`. Forwarding of traps is supported, with filtering by source address.

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

User and group information for v3 connections must be different from the user and groupnames used for accessing the OnBoard appliance for the following reasons:

- To keep the OnBoard appliance user information more secure, since SNMP usernames and passwords are stored in cleartext in `/etc/snmp/snmpd.conf`
- To allow different users and groupings to be used for SNMP access

The administrator can configure the following:

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

OnBoard appliance traps occur on the following types of events:

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

Traps are handled the three following ways:

- When access is through a VPN tunnel, the public-side computer directly receives SNMP traps from the connected device
- SNMP traps can be forwarded to SNMP agents based on the source address of the trap
- Locally, traps are sent to the syslog facility, which may use the information to send notifications

Before enabling SNMP, depending on the version of SNMP in use, the administrator needs some or all of the information in the following table.

Table 4.10: Values for Configuring SNMP

Values	Description
SysContact	Email address of the OnBoard appliance administrator
SysLocation	Location of the OnBoard appliance

Table 4.10: Values for Configuring SNMP (Continued)

Values	Description
OID	Object Identifier. A unique identifier 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 Internet Engineering Task Force (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 version (also called protocol)	<ul style="list-style-type: none"> • v1-Uses a community string match for authentication • v2c-Uses a community string match for authentication • v3-Uses a username for authentication. In addition to the username, an optional authentication password may be used. An encryption password also may be used for encrypting traffic. Cyclades recommends that both authentication and encryption be used to maximize the security of data and commands. Available authentication methods are MD5 or SHA. Available encryption methods are DES and AES.
Community	For SNMP v1 and v2c only the community name is used for authentication. An arbitrary string, with a maximum length of 256 characters. Does not need to match the community name used on the public side or be unique on the private side. Must match the community string expected by the device, often public.
Source	For SNMP v1 and v2c only. <ul style="list-style-type: none"> • Default • Use IP-Enter an IP for the source device in the field if you select this option. If the default is selected, then all traps from all source IPs are forwarded to the destination IP.
For configuring SNMP v3 only:	
Auth Level/Security level	No auth-Applies to v1 and v2c by default and is an option in v3 Auth Auth & crypt
User name	Username to be used for authentication.
Auth method	<ul style="list-style-type: none"> • MD5 • SHA
Auth pass	Optional password used for authentication. Must be either empty or at least eight characters.
Encryption	<ul style="list-style-type: none"> • DES • AES
Crypt pass	Optional password used for encryption. Must be either empty or at least eight characters. If used, an authentication password is required.

Strings are defined as case-sensitive ASCII, not beginning with a hash and delimited by a space, form-feed ('\f'), newline ('\n'), carriage return ('\r'), horizontal tab ('\t'), vertical tab ('\v') or null ('\0'). Any character may be included if it is escaped with a backslash ('\'). Two backslashes are interpreted as one.

Views can be created to define 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 describes the values used for configuring views.

Table 4.11: Values for Configuring an SNMP Trap Notification

View name	Administratively-assigned name
OID: Include or Exclude	Object Identifier. A unique identifier 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 Internet Engineering Task Force (IETF), which grants authority for parts of the OID name space to individual organizations.
Mask: Include or Exclude	Mask that defines a view subtree. Can be all ones, all zeros or a combination of both. Default = ff.

The following table describes the values used for configuring SNMP traps.

Table 4.12: Values for Configuring an SNMP Trap Notification

For configuring SNMP traps only:	Options
Generic trap type	coldStart warmStart linkDown linkUp authenticationFailure egpNeighbor Loss enterpriseSpecific
Server	The IP address or DNS name of the SNMP manager
Body	The text you want sent in the trap message

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

Table 4.13: Tasks for Configuring SNMP

Task	Where Documented
Configure SNMP	<i>Configuring SNMP</i> on page 161 <i>To configure SNMP trap notifications:</i> on page 153 <i>To configure an SNMP trap sensor alarm action:</i> on page 158 <i>To configure an SNMP trap sensor alarm action:</i> on page 158 <i>To begin configuring SNMP for a device:</i> on page 164 <i>To configure a device's SNMP settings:</i> on page 164 <i>To configure a device's SNMP access settings:</i> on page 164 <i>To configure users with SNMP v3:</i> on page 165 <i>To configure views with SNMP v3:</i> on page 165 <i>To configure security with SNMP v3:</i> on page 165 <i>To configure SNMP trap forwarding:</i> on page 166
Activate the SNMP service	<i>To configure services:</i> on page 169

VPN on the OnBoard Appliance

As described in the Cyclades OnBoard Service Processor Manager User Guide, for security reasons an authorized user must establish a trusted connection with the OnBoard appliance before gaining native IP access to native management features on connected SPs.

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 appliance 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 appliance 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 appliance take care of encryption and decryption on their end. See *Configuring VPN Connections* on page 70 for more information.

Message Logging (With Syslog) on the OnBoard Appliance

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

- Events of interest from the OnBoard appliance
- Events of interest obtained by filtering data during device console connections with connected devices

- Overcurrent status from a connected Cyclades 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 (Emergency)
- 1 - ALERT
- 2 - CRIT (Critical)
- 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.

Tasks for configuring syslog messages

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

Table 4.14: Tasks for Configuring Syslog Messages

Task	Where Documented
Specify one or more syslog servers, optional additional destinations for syslog messages and configure message filtering	<i>To configure the Syslog destination and message filtering: on page 167</i>
Specify sensor alarms to be sent as syslog messages	<i>To begin configuring a sensor alarm: on page 156</i> <i>To configure a Syslog message sensor alarm action: on page 157</i> <i>To configure an SNMP trap sensor alarm action: on page 158</i> <i>To configure a pager sensor alarm action: on page 159</i> <i>To configure an email sensor alarm action: on page 160</i>
Specify overcurrent alerts to be sent as syslog messages	<i>To enable overcurrent protection for an IPDU: on page 121</i>

Ethernet Ports on the OnBoard Appliance

The OnBoard appliance's two public Ethernet ports are used for connecting to the public (or management) network. The managed private side of the OnBoard appliance 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 appliance 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 private Ethernet ports.

Each private Ethernet port may be connected to multiple SPs. For example an Ethernet port may be connected to a blade manager that has multiple SPs, 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 appliance, 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 appliance 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 `HWaddr` [MAC address] and `inet addr` [IP address] are identical for `bond0`, `eth0` and `eth1`.

```
[root@ONB /]# ifconfig
```

```
bond0Link 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
```

```
eth0Link 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
...
eth1Link 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
```

For more information, see the following sections.

- *Configuring network interfaces* on page 99
- *To configure OnBoard appliance network interfaces:* on page 102
- *Configuring network interfaces* on page 99

Dial-in and Callback Access to the OnBoard Appliance

The OnBoard appliance administrator can configure dial-in or callback access to the OnBoard appliance using PPP through either an external modem connected to the modem port or to a PC modem, GSM or CDMA card. PC modem and phone cards can also be accessed for logins without PPP from a terminal emulation program.

The following table lists the modem and phone card configuration tasks, with links to where they are documented.

Table 4.15: Tasks for Configuring Dial-ins and Installing Modems

Modem Type	Where Documented
External modem	<ul style="list-style-type: none">• <i>To connect an external modem to the AUX port:</i> on page 20• <i>Configuring the AUX port for a modem</i> on page 115
PC modem card	<ul style="list-style-type: none">• <i>To install a PCMCIA card:</i> on page 19

NOTE: Administrators can also configure modems through the `cycli` utility. See *Configuring Dial-ins Using cycli* on page 74 for examples.

Table 4.16 shows the configuration options that apply whether a modem or phone card is being configured through the Web Manager or the cycli utility.

Table 4.16: Modem and Phone Card Field and Menu Options

Field or Menu Option/cycli parameter	Options/cycli parameter	Notes
Access Type/type	<ul style="list-style-type: none"> Autodetect/autopp Login/login PPP/ppp OTP/otlogin 	<ul style="list-style-type: none"> Autodetection means that either type of access (PPP or Login) may be automatically detected. When autodetect is selected in the Web Manager, all the fields for configuring PPP and Login appear on the same screen and must be filled out. When autopp is set using cycli as the modem access type, then the PPP options should be configured. OTP/otlogin supports OTP authentication for only login access only to modem or GSM or CDMA PCMCIA cards
Baud Rate/speed	300 to 460800	Default = 9600
Flow Control/data-flow	Flow Control/data-flow	Default = none
Modem Initialization/initchat	A modem initialization string (or chat string) of AT commands used to configure the modem or phone when it is turned on or when the communications software dials out to another modem or phone.	<p>Example: initchat ATZ OK</p> <p>A longer example: TIMEOUT 10 \d\d\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</p>
Callback/ cbphone_enable, cbphone	If callback is selected, a callback number must be entered.	

Power Management Options on the OnBoard Appliance

Authorized users and OnBoard appliance administrators can power down, power up and reboot devices with IPDU or SP power management.

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

Table 4.17: Tasks for Configuring Power Management

Task	Where Documented
Configure IPDU power management by doing the following: <ul style="list-style-type: none"> • Connect one or more Cyclades PM IPDUs to the AUX port • Configure the AUX port for IPDU power management • Configure users for IPDU power management 	<ul style="list-style-type: none"> • <i>Connecting One or More IPDUs to the AUX Port</i> on page 21 • <i>Configuring the AUX port for IPDU power management</i> on page 115 • <i>Configuring users to manage power outlets on a connected IPDU</i> on page 121
Configure users for SP power management	<i>Configuring regular users</i> on page 108

Adding Options to the User's Console Login Menu

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 appliance's console. The OnBoard appliance administrator can configure the `rmenush` menu to display other options including links to additional submenus or commands by modifying the `/etc/menu.ini` file. See *Configuring the User's Console Login Menu* on page 78 for more information.

Routing on the OnBoard Appliance

The OnBoard appliance administrator can configure routing for default, host or network routes using either the Web Manager or the `cycli` utility.

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, the gateway IP is used to create a default route.

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 route and provides links to where the tasks are documented.

Table 4.18: Tasks for Configuring Routes

Task	Where Described/Description
Configure a default route (Web Manager)	<ul style="list-style-type: none"> • <i>Configuring network interfaces</i> on page 99 • <i>To configure OnBoard appliance network interfaces:</i> on page 102
Configure a host or network route (Web Manager)	<ul style="list-style-type: none"> • <i>Configuring static routes</i> on page 178 • <i>To add a static route:</i> on page 179
Configure default, host or network routes (cycli)	<ul style="list-style-type: none"> • <i>Configuring routes</i> on page 100 • <i>To configure routes with cycli:</i> on page 79

OnBoard Appliance Notifications

The OnBoard appliance includes syslog-ng, which can be configured through either the Web Manager or the cycli utility to filter log messages sent by system daemons (such as messages from the cron daemon, crond) and by connected devices. By default, the `/etc/syslog/syslog-ng.conf` file monitors messages from the following two files:

- `/dev/log`
- `/proc/kmsg`

Notifications can be configured to be sent to an OnBoard appliance administrator by one of the following methods:

- SNMP trap
- Pager
- Email

syslog-ng allows administrators to set up additional alarm triggers to filter messages based on the messages' facility, level or contents.

Alarm triggers must be specified in the following format:

```
function('one_or_more_criteria_connected_by_operators');
```

Supported operators are and, or and not.

The following line shows the syntax for a match function.

```
match('regular_expression_matching_a_text_string');
```

The following line shows the syntax for two match functions connected by the not operator.

```
match('regular_expression') and not match("regular_expression');
```

The following example shows the two match functions filtering for logins and excluding messages that have the username francisco; the functions are connected by the not operator.

```
match('[Ll]login') and not match("francisco');
```

See the syslog-ng v1.6 reference manual at <http://www.balabit.com/products/syslog-ng/reference-1.6/syslog-ng.html/index.html#filterfunc> for more information.

See the following sections for how administrative users can configure notifications and alarms and email:

- *Configuring Notifications* on page 152
- *Configuring Sensor Alarms* on page 155
- *Configuring outbound email* on page 135

OnBoard Appliance Sensor Alarms

The OnBoard appliance may also be configured to periodically check sensor readings from SPs and to send alarms based on specified sensor values, using either the Web Manager or the cycli utility. Alarms can be configured to be sent to OnBoard appliance administrators by one of the following methods:

- Syslog message
- SNMP trap
- Pager
- Email

The following table shows the fields for configuring sensor alarms.

Table 4.19: Values for Configuring Sensor Alarms

Values	Description
Device	Choose from a list of all configured devices.
Sensor	The literal string for the sensor (which can be obtained from the sensor logs from the device), for example, Sys Fan 1.
Condition	<ul style="list-style-type: none">• Trigger when value is >INSIDE< range.• Trigger when value is <OUTSIDE> range.• Trigger when value CHANGES.
Range	Applies to the INSIDE and OUTSIDE conditions. The low and high thresholds can be any numeric value, including floats. For example, for a fan whose average reading is 1470 RPR, you might want to specify a low threshold of 1000 and a high threshold of 1600.

Table 4.19: Values for Configuring Sensor Alarms (Continued)

Values	Description
Interval	A polling interval chosen by the administrator: a time in minutes or hours.
Action	<ul style="list-style-type: none"> • Syslog message trap. • Pager. • Email.
Comment	Any desired comment to identify the source of the alarm.

See *Configuring Sensor Alarms* on page 155 for how to configure sensor alarms through the Web Manager. See *sensoralarm* on page 220 for `cycli` command instructions.

Device Configuration

When connecting devices to the OnBoard appliance, observe the following recommendations, which are illustrated in Figure 4.1:

- Connect the dedicated Ethernet port on each SP or device to one of the OnBoard appliance's private Ethernet ports.
- Connect the OnBoard appliance's primary Ethernet port (`eth0`) to a local management network and usually to the Internet

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

Figure 4.1 illustrates connecting two servers that have SPs, with the SPs indicated by gray boxes. (The same recommendations apply to connecting devices that do not have SPs but that have dedicated Ethernet ports that provide access to the devices' consoles.)

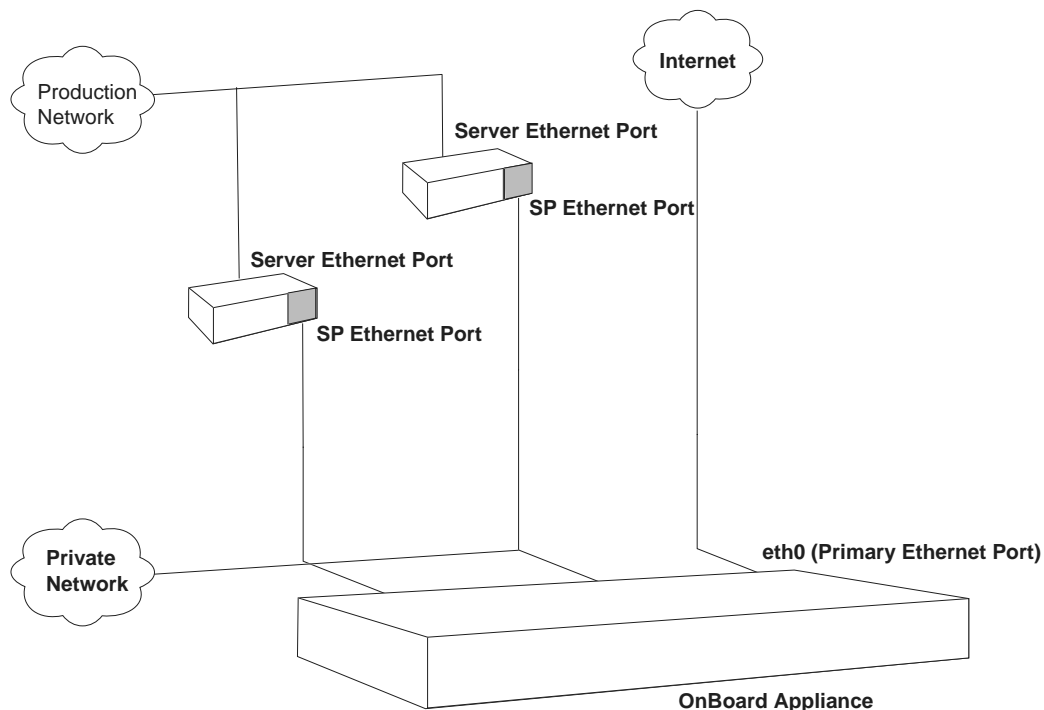


Figure 4.1: Recommended Device Configuration

Preparing an addressing scheme

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

As illustrated in Figure 4.1, the dedicated Ethernet ports on SPs and on other supported types of devices are connected to the private Ethernet ports on the OnBoard appliance. 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 appliance side.

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

- Devices when talking to the private Ethernet ports of the OnBoard appliance
- Users who make PPTP or IPsec VPN connections to enable native IP access

Figure 4.2 shows some example IP addresses assigned.

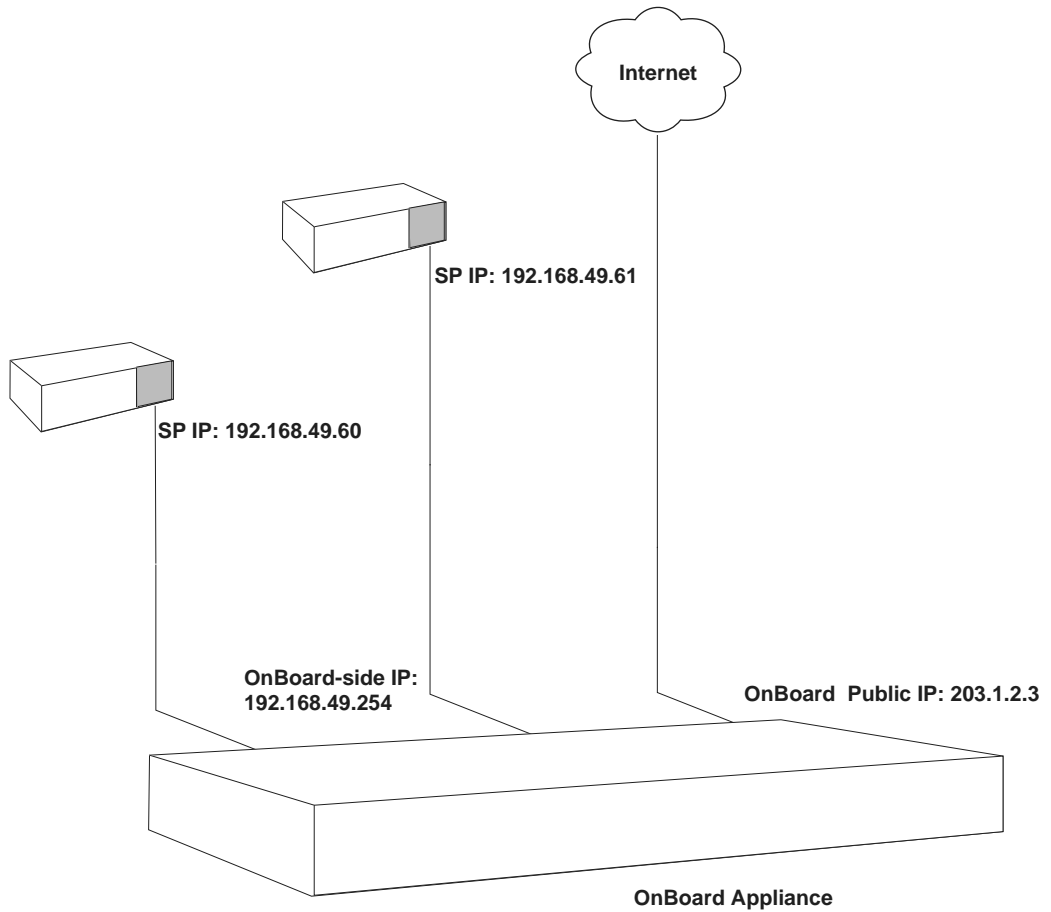


Figure 4.2: IP Addressing Example

See *Address configuration for connected devices* on page 247 for the details needed for planning and implementing IP addresses.

Parameters for configuring devices

The OnBoard appliance 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 4.20: 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 Cyclades OnBoard Service Processor Manager User 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 username and password pair that the user enters to access the appliance.
Device group	If an OnBoard appliance administrator has configured one or more device groups, the device can be assigned to a device groups.
Type	The type of service-processor-management protocol or type of access. The following lists each of the defined SP and device types. <ul style="list-style-type: none"> • iLO • RSA II • DRAC • IPMI 1.5 • device console • custom1 • custom2 • custom3 See <i>Device type differences</i> on page 231 for more information about assigning the correct device type.
Data buffering	Options for data buffering for the device are Yes, No, or Default.
Private subnet	Used by the OnBoard appliance to communicate with devices on the private network. See <i>Private Subnets on the OnBoard Appliance</i> on page 51 and <i>Why define private subnets?</i> on page 249 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: <ul style="list-style-type: none"> • <i>Configuring private subnets and virtual addresses</i> on page 103 • <i>Configuring private subnets and virtual networks</i> on page 182.

Table 4.20: Device Configuration Parameters (Continued)

Parameter	Description
Device IP address	An IP address used by the OnBoard appliance to communicate with the device. See <i>Preparing an addressing scheme</i> on page 48, <i>Address configuration for connected devices</i> on page 247 and <i>Options for assigning IP addresses to connected devices</i> on page 271 for more information about assigning IP addresses.
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, SP console or device console access cannot be prevented from discovering the IP address of the dedicated Ethernet port that is connected to the OnBoard appliance.) Virtual addresses are available only if a virtual network has been configured using DNAT. See <i>Why define virtual (DNAT) addresses?</i> on page 264 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 appliance, unless SSH tunneling is used to create a secure path for users who are authorized for native IP access. When an SSH tunnel is used, the OnBoard appliance and the device must be using the same authorization method. See <i>OnBoard Appliance Authentication Options</i> on page 24. See also Table 4.2 on page 25 for a detailed list of authentication types supported for devices.
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 that perform device management actions.

NOTE: The OnBoard appliance has been tested with the SP and device types and firmware versions listed in the release notes. If the firmware on an SP being managed by the OnBoard is at another level, or if the SP is not listed in the release notes, the administrator needs to follow the instructions in Appendix C: Device Configuration to configure support for the device.

Private Subnets on the OnBoard Appliance

Connected devices should be isolated (as recommended under *Device Configuration* on page 47) on a management network that is separate from the production network and from the public network. With the recommended configuration, the OnBoard appliance 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 appliance

If a device is not assigned a private subnet, the OnBoard appliance 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 appliance.

For more details about setting up subnets, see *Address configuration for connected devices* on page 253.

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* on page 103 and *Configuring private subnets and virtual networks* on page 182.

Tasks for Configuring IP Addresses

See *Tasks for configuring new devices* on page 230.

Example and Demo Scripts

The following helps are available for OnBoard appliance administrators:

- Configuration example scripts in `/libexec/example_scripts`
- Demo scripts in `/libexec/demo_scripts`

Data Buffering on the OnBoard Appliance

The OnBoard appliance supports the buffering (storing) of data from the consoles of connected devices so that the data can be monitored to detect events of interest and, when appropriate, generate alarms. Enabling data buffering can be done through the Web Manager or by using the `cycli` utility. Configuring where data buffer files are stored must be done manually.

Enabling data buffering

The administrator can configure a default for data buffering and then configure each device to use the default or not. An administrator can configure data buffering either by using the Web Manager or by using the `cycli` utility as described in the following sections:

- *Configuring devices* on page 106 and *onboard global default databuf* on page 219
- *onboard server* on page 220

Configuring where buffered data is stored

By default the buffered data is stored in RAM. The administrator may manually configure the storage of data either on a directory mounted from an NFS file server or on a PC Flash memory card. See *Configuring Storage of Buffered Data* on page 57.

Firewall/Packet Filtering on the OnBoard Appliance

Packet filtering on the OnBoard appliance is controlled by chains and rules that are configured in iptables. (For more details about the predefined chains and rules, see *Chains* on page 53 and *Rules* on page 53.)

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

- Because the OnBoard appliance 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 appliance 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.

CAUTION: It is possible for an OnBoard appliance administrator to create rules that circumvent the access controls on a device.

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 appliance 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 appliance's private Ethernet ports and devices on the public side of the OnBoard appliance. 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 are in the iptables filter table: INPUT, OUTPUT and FORWARD.

These three chains are in the nat table: PREROUTING, POSTROUTING and OUTPUT. 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:

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 4.21: Filter Options for Packet Filtering Rules

Filter Options	Description
Protocol	You can select a protocol for filtering from one of the following options: <ul style="list-style-type: none"> • ALL • TCP • UDP • ICMP • GRE • ESP • AH
Source IP/mask Destination IP/mask	A host IP address or subnetwork IP address in the form: <i>host/IPaddress</i> or <i>network/IPaddress/NN</i> . 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: <ul style="list-style-type: none"> • Public 1 (eth0) • Public 2 (eth1) • Failover (bond0) • PCMCIA (eth2) • PCMCIA (eth3) • Any private port (priv0)
Fragments	The types of packets to be filtered: <ul style="list-style-type: none"> • All packets and fragments • Head fragments and unfragmented packets • Non-head fragments only
Rule target	<ul style="list-style-type: none"> • Accept • Drop • Reject

Any of the options in Table 4.21 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 specify packet filtering by adding new rules for existing chains and editing or deleting 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 4.22: Tasks for Configuring Packet Filtering (Firewall) Rules

Task	Where Documented
Add a new rule, edit or delete a customer-added rule	<ul style="list-style-type: none"> • <i>Configuring firewall rules for packet filtering</i> on page 174 • <i>To add a new packet filtering (firewall) rule:</i> on page 176 • <i>To edit an administrator-added packet filtering (firewall) rule:</i> on page 176

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

How Configuration Changes Are Handled

The following bulleted items give an overview of how the Cyclades OnBoard Service Processor Manager handles configuration changes:

- When an 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 administrator can back up changed configuration files at any time.
- The OnBoard appliance maintains a backed up copy of the factory-default configuration files.
- The administrator can restore the factory default configuration files or restore any backed-up copies of the configuration files.
- The current state of the configuration files is maintained after a software upgrade. (This allows you to upgrade software on the OnBoard appliance without losing all user and device configurations.) After a software upgrade, the administrator can optionally do the following:
 - Return from the current state to the last backed-up copy of the configuration files.
 - Return to the factory default configuration files.
- When an administrator adds a new application, script or configuration file to the system, the root user needs to add the pathname to the file to the list of files to be backed up and restored.

The following table shows tasks for administrators to save changes to configuration files and back up configuration files and provides links to where they are documented.

Table 4.23: Tasks for Saving Changes, Backing Up and Restoring Configuration Files

Tasks	Action
Saving configuration file changes	<ul style="list-style-type: none">• <i>Saving Configuration Changes</i> on page 81• <i>To save configuration changes:</i> on page 81
Backing up configuration files	<ul style="list-style-type: none">• <i>Backing Up Configuration Files</i> on page 81• <i>To back up configuration files:</i> on page 81
Restoring backed-up configuration files	<ul style="list-style-type: none">• <i>Restoring Backed Up Configuration Files</i> on page 82• <i>To restore the OnBoard appliance configuration files to the last saved version:</i> on page 82
Restoring factory default configuration files	<ul style="list-style-type: none">• <i>Restoring Factory Default Configuration Files</i> on page 82• <i>To restore the factory default configuration files from the command line:</i> on page 82
Adding new files to be backed up and restored	<ul style="list-style-type: none">• <i>Adding New Files to Be Backed Up and Restored</i> on page 82• <i>To configure an added script or other file for backup and restoration:</i> on page 82

Administration Tasks Not Performed in the Web Manager

This section lists the configuration and maintenance tasks that are performed by an administrator (either the root user, the admin user, or a member of the admin group) either on the Linux command line, using the `cycli` utility or in the U-Boot monitor mode.

Configuring Storage of Buffered Data

If data buffering is enabled, console output from managed devices is sent to the `syslog` daemon but is not stored. This section describes how the root user can manually configure the storage of buffered data either in a directory mounted from an NFS file server or in a PC Flash memory card.

Table 5.1: Configuration Files Used in Data Buffering

File	Use
<code>/etc/fstab</code>	If using an NFS-mounted directory for storage, modify the <code>/etc/fstab</code> file to define the NFS mount point. NOTE: This file does not need to be edited for mounting a compact Flash PCMCIA card, because a compact Flash card is detected and automatically mounted under the <code>/mnt</code> directory when the OnBoard appliance is rebooted after card installation.
<code>/etc/syslog-ng/syslog-ng.conf</code>	Device data received by the OnBoard appliance is sent to the <code>syslog-ng</code> daemon, which uses this file. This file can be modified to configure buffered data from all devices to be stored in a single file. See <i>To store buffered data in multiple files, one for each connected device</i> : on page 58.
<code>/usr/sbin/cyc-conserver</code>	Determines what is inserted into the <code>conserver.cf</code> file when a new device is added. This file can be modified to configure buffered data from each device to be stored in a separate file. See <i>To store buffered data in multiple files, one for each connected device</i> : on page 58. NOTE: The <code>/usr/sbin/</code> directory is mounted read-only by default. The procedure describes how you can mount the <code>/usr/sbin/</code> directory in read-write mode before you can edit the <code>cyc-conserver</code> file.
<code>/etc/conserver.cf</code>	Determines where data buffer files are stored. Because direct user modifications to <code>conserver.cf</code> are lost whenever a new device is added, the <code>cyc.conserver</code> file is modified instead.

To store buffered data in a single file:

1. Log into the OnBoard appliance's console as root.
2. Add the following entries to the syslog-ng.conf file.

The example entries configure data buffer storage in an NFS-mounted /mnt/nfs_server/log/device.log file.

```
source src_dev_log { unix-stream("/dev/log"); };  
filter f_device { program("conserver");};  
destination d_device { file("/mnt/nfs_server/log/device.log"); };  
log { source(src_dev_log); filter(f_device); destination(d_device); };
```

3. Put the syslog-ng.conf file changes into effect by stopping and restarting syslog-ng, as shown in the following command line.

```
$ killall -hup syslog-ng
```

The configuration changes are saved to the appliance's resident Flash memory if the appliance is booted from a local image.

To store buffered data in multiple files, one for each connected device:

1. Log into the OnBoard appliance's console as root.
2. Use the **cat** command to display the contents of the /proc/cmdline file to find out which boot image is currently running.

```
[root@OnBoard /]# cat /proc/cmdline  
root=/dev/hda6 console=ttyS0,9600
```

If the output shows root=/dev/hda5, Image 1 is running, and if root=/dev/hda6, Image 2 is running.

3. Mount the directory for the running image with read-write permission.

```
$ mount -t ext2 -o rw,remount /dev/hda5
```

-or-

```
$ mount -t ext2 -o rw,remount /dev/hda6
```

4. Open the /usr/sbin/cyc-conserver file for editing.

```
$ cd /usr/sbin  
$ vi cyc-conserver
```

5. Change the variable LOGDIR to the pathname of the directory where you want the data buffer files to be stored.

```
'LOGDIR=/mnt/nfs_server/log'
```

-or-

```
'LOGDIR=/mnt/pc_compact_flash_card/log'
```

6. Remove the following line.

```
llset('conserver', "server/$server/logfile", "/dev/null"),
```

7. Ensure the following line is still present or enter it in place of the deleted line above:

```
llset('conserver', "server/$server/logfile", "$server.log"),
```

NOTE: This example configuration stores the buffered data in separate files according to each device's alias. Adding devices automatically results in their data being buffered to a device-specific logfile.

Using MindTerm to Create an SSH Tunnel

This section describes how an administrative user can create an SSH tunnel from a remote workstation to a managed device using the MindTerm applet that activates when any user connects to the OnBoard appliance console using the Web Manager. A regular user cannot use the procedure because regular users who connect to the OnBoard appliance's console are restricted to selecting options from a limited-access menu and the Tunnels option is not available for them on the MindTerm menu.

To use MindTerm to create an SSH tunnel:

1. Click the *Access-Connect to OnBoard* menu option on the Web Manager as an administrative user. A window running a MindTerm applet appears, with an encrypted SSH connection between the user's computer and the console.
2. Log in and follow any prompts that may appear about saving the host key.
3. Press **Ctrl** and the third mouse button at the same time (**Ctrl**+**[mouse right-click]**) then drag the cursor to pull down and select the Tunnels-Basic menu option.

The MindTerm Basic Tunnels Setup dialog appears.

4. Enter a TCP port number to forward in the Local port field. You can select a random number over 1000.
5. Enter the device's port number to bring up the desired web application in the Remote port field.
6. Enter the IP address of the device in the Remote Host field.
7. Click *Add*.

The tunnel is created and the dialog appears similar to the following screen example.



Figure 5.1: MindTerm Basic Tunnels Setup Dialog

Specifying the Location for the OTP Databases

As configured on the OnBoard appliance, OTP expects its user databases to reside in `/mnt/opie/etc`. The OnBoard appliance's resident Flash memory does not provide a directory for the OTP databases. Onboard administrator must mount a device on `/mnt/opie`. You may use a compact Flash PCMCIA card or an NFS-mounted directory.

To configure a compact Flash card for OTP, the root user logs into the OnBoard appliance's console and runs the `/bin/do_create_cf_ext2` script on the command line. The script does the following:

- Creates a partition on the compact Flash (`sfdisk /dev/hdc`)
- Creates an ext-2 filesystem on the compact Flash (`mke2fs /dev/hdc1`)
- Mounts the compact Flash on the `/mnt/opie` directory (`mount -t ext2 /dev/hdc1 /mnt/opie/`)
- Creates the directory `/mnt/opie/etc`
- Creates the file `/mnt/opie/etc/opiekeys`
- Sets the permissions of the file to mode 0644, the owner of file to root and the group to bin
- Creates the directory `/mnt/opie/etc/opielocks` for the OPIE lock files
- Sets the permissions of this directory to 0700 and the owner and group to root

To configure a PC compact Flash card for OTP database storage:

1. Log into the OnBoard appliance console as root.
2. Enter the `/bin/do_create_cf_ext2` script on the command line.

To configure a NFS-mounted directory for OTP database storage:

1. Make sure a directory (for example /home/opie), has been created on the NFS server and is shared (exported) via NFS.
2. Log into the OnBoard appliance console as root.
3. Enable the RPC service using the **cycli** utility.

```
[root@OnBoard /]# cycli -CF set service rpc enable yes
```

4. Mount the directory from the NFS server.

The following screen example uses `nfs_server.avocent.com` as the NFS server name and `/home/opie` as the exported directory's name.

```
[root@OnBoard /]# mount -t nfs nfs_server.avocent.com:\
/home/opie /mnt/opie
```

5. Enter the following commands to create the `/etc` directory on the mounted directory and to create an `opiekeys` file.

```
[root@OnBoard /]# mkdir /mnt/opie/etc
[root@OnBoard /]# touch /mnt/opie/etc/opiekeys
[root@OnBoard /]# chmod 0644 /mnt/opie/etc/opiekeys
[root@OnBoard /]# chown root:bin /mnt/opie/etc/opiekeys
```

To configure OTP authentication for modem or GSM phone card dial-ins:

1. Log into the OnBoard appliance console as root.
2. Use **vi** or another text editor to open the `/etc/mgetty.login.config` file for editing and find this entry: `* - - /bin/login`.

```
[root@OnBoard /]# vi /etc/mgetty.login.config
...
*      -      -      /bin/login @
```

3. Replace `login` with `opielogin`.

```
*      -      -      /bin/opielogin @
```

4. Save and quit the file.

To configure OTP authentication for SSH or console logins:

This procedure manually configures Telnet or SSH logins to the console with either the OTP or OTP/Local authentication method, and it also changes the targets of the symbolic links `/etc/pam.d/sshd` and `/etc/pam.d/login` to `/etc/pam.d/[otp,otplocal]`.

NOTE: The Web Manager does not support OTP authentication.

1. Change to the /etc/pam.d directory.

```
[root@OnBoard /]# cd /etc/pam.d
```

2. To specify OTP for logins to the console or through telnet, change the target of the symbolic link login to otp or otplocal.

CAUTION: If OTP is chosen, users (even root) may be locked out if not configured properly. You can test whether OTP is working by first changing only the symbolic link for login as shown in the following screen example and then attempting access using telnet. If the telnet login using an OTP password succeeds, you can safely change the method for ssh logins as described in step 3.

```
[root@OnBoard /]# ln -sf /etc/pam.d/otp login
```

-or-

```
[root@OnBoard /]# ln -sf /etc/pam.d/otplocal login
```

3. To specify OTP for ssh logins, change the target of the symbolic link sshd to otp or otplocal.

```
[root@OnBoard /]# ln -sf /etc/pam.d/otp sshd
```

-or-

```
[root@OnBoard /]# ln -sf /etc/pam.d/otplocal sshd
```

NOTE: The cycli utility and the Web Manager may not display the correct authentication information when the symbolic links are changed manually.

To configure OTP authentication for a device:

This procedure manually configures a previously-configured device or devices to use the OTP or OTP/Local authentication method.

1. Log into the OnBoard appliance's console as root.
2. Open the /etc/onboard_server.ini file for editing.
3. For any configured device, set the authtype to be either otp or otplocal.

```
authtype = otp
```

-or-

```
authtype = otplocal
```

4. Save and quit the file.

How Users are Registered with OTP and Obtain OTP Passwords

All users who need to use OTP authentication must have a local account on the OnBoard appliance, must be registered with the OTP system and must be able to obtain OTP passwords.

The OPIE commands in the following bulleted list must be executed with the -c option while the user is logged in locally through the OnBoard appliance's console port:

- The `opiepasswd` command
- The `opiekey` command to generate OTP passwords

The requirement for local logins through the console port is enforced for regular users because running the commands through a dial-in or other unsecure connection may expose the user passwords, pass phrases and OTP passwords. The root user can execute these commands without the `-c` option while logged in over ssh because ssh provides a secure path. These commands should never be executed over a dial-in or telnet connection:

OTP passwords are generated in one of the two following ways:

- By the user or administrator executing the `opiekey` command: If `opiekey` command is executed by an administrator on behalf of a user, the administrator must give the OTP username and the user's secret pass phrase to each user along with the generated OTP passwords
- By the user with a password generating device: If a user has a password generating device, then the user generates the OTP password when challenged at login using the username and secret pass phrase, along with the seed and sequence number that are displayed along with the OTP challenge.

To register and generate OTP passwords for users:

The following procedure shows an example of an administrator logging in locally through the console port, registering a user and generating OTP passwords for the user. The example shows using `cycli` to add the user, but any of the tools available for adding users, including the Web Manager, may be used to configure the user account beforehand.

1. Log into the OnBoard appliance console as root.
2. Make sure each user authorized for dial-ins has a local account on the OnBoard appliance.

If using the `cycli` utility to add the user, do the following steps.

- a. Add the user and set the user's password.

The following screen example shows using the `cycli` utility to add user joe and set the user's password to `joes_passwd`.

```
[root@OnBoard /]# cycli
cli> add user joe
OK
cli> set user joe passwd joes_passwd
OK
```

- b. If the user needs to access devices through the OnBoard appliance, add the user as an onboard user.

NOTE: Adding users through the Web Manager adds them as normal UNIX users and as onboard users without requiring a separate step.

```
cli> add onboard user joe
```

```
OK
```

- c. If you are using cycli, commit the changes.

```
cli> commit
```

```
OK
```

```
cli> exit
```

```
[root@OnBoard /]#
```

3. Enter the **opiepasswd** command to register the user.

The following example shows using **opiepasswd** with the **-c** option while logged in locally through the OnBoard appliance console port. If you are logged into the OnBoard appliance's console using **ssh**, do not use the **-c** option. The example uses **joe** as the username and **joes** secret pass phrase as the secret pass phrase.

NOTE: The secret pass phrase is not the same as the user's regular login password.

In the example, the **opiepasswd** command generates a default OPIE sequence number of 499 and a creates a seed (or key) from the first two letters of the hostname and a pseudo random number, in the example **on93564**.

```
[root@OnBoard /]# opiepasswd -c joe
```

```
Adding joe
```

```
Reminder - Only use this method from the console; NEVER from remote. If you are using telnet, xterm, or a dial-in, type ^C now or exit with no password. Then run opiepasswd without the -c parameter. Using MD5 to compute responses.
```

```
Enter new secret pass phrase: joes secret pass phrase
```

```
Again new secret pass phrase: joes secret pass phrase
```

```
ID joe OPIE key is 499 on93564
```

```
CITY MARY GLOW BILL MAY ARM
```

```
[root@OnBoard /]#
```

4. If desired, enter **opiekey** to generate a number of passwords for the user.
5. Give the OTP username, secret pass phrase and any OTP passwords generated in this procedure to the user.

6. Save the changes by entering the **saveconf** command.

Configuring SSH or Bidilink Instead of Telnet for Device Connections

The root user can replacing Telnet with SSH or bidilink, as described in the following procedure.

To substitute SSH or bidilink for Telnet for device connections:

1. Log into the OnBoard appliance console as root.
2. Change to the `/libexec/onboard` directory.
3. To begin configuring bidilink as the device connection method, perform the following steps.
 - a. Copy `bidi_login.exp` to a new file named `soe_login.exp`.

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

```
[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 screen example shows the line to change.

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

This example shows the comment (#) sign removed and PORT changed 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 appliance 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]] "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]] "ssh_login.exp"]
```
  8. Save and quit the file.

9. Assign the new custom type to the appropriate SPs. For example, if you have created a `talk_custom1.exp` for iLO SPs, configure the iLO SPs as `custom1` type. If you are substituting `bidilink`, you are done.
10. If you are substituting `ssh`, set up host keys for every SP configured to use `ssh` by doing the following steps.
  - a. Use **ssh** to connect to the SP as an administrator.

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

A prompt 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 SP, enter **yes**.
- c. Enter the password when prompted.

## Replacing the Self-Signed Certificate With an SSL Certificate for HTTPS

As described in *HTTPS on the OnBoard Appliance* on page 34, an OnBoard appliance administrator needs to replace the automatically-generated self signed certificate with an SSL certificate from an official certificate authority. The root user can follow the instructions in the following procedure to generate a certificate signing request; after obtaining the certificate from the CA, the root user then needs to install the public key and the certificate in the Apache web server on the OnBoard appliance.

### To replace the self-signed certificate with one from a certificate authority:

1. Log into the OnBoard appliance 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.

```
[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 5.2: 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.                     |
| 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 Widges 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.crt - /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.
7. Restart the web server to put the certificate into effect.

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

## 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 appliance's 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 appliance 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 in the pasted section.

```
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 host MySP line and replace MySP with a hostname/alias for the device.
  - b. Specify the MAC address of the device on the line that begins hardware ethernet.
  - c. Specify the desired IP address for the device on the line that begins fixed-address.



For example, see the following edited host entry.

```
host spl {
 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.
10. Save and quit the file.
11. Save the configuration file changes by entering the **saveconf** command.
12. Start dhcpd by either restarting the OnBoard appliance or restarting dhcpd.

The following screen example shows the syntax for restarting dhcpd.

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

## Configuring VPN Connections

This section describes what the administrator must do to enable VPN on the OnBoard appliance side to enable users to create VPN tunnels to the OnBoard appliance; VPN tunnels are required for a user to obtain native IP access through the Web Manager or through entering ssh with the nativeipon device management command. The OnBoard appliance administrator must do the tasks shown in the following table.

**Table 5.3: 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). | <i>OnBoard Appliance Services</i> on page 32                                                                                              |
| Configure a VPN connection profile on the OnBoard appliance for the type of VPN connections that are being used. | <i>Configuring VPN connections</i> on page 179<br>Also see examples under: <i>Address configuration for connected devices</i> on page 247 |

The user's workstation must have support for either IPsec or PPTP VPN. The user must do the tasks in the following list to configure a VPN tunnel:

- Obtain from the OnBoard appliance administrator the values used in creating the VPN connection profile on the OnBoard appliance 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 appliance 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 appliance, the user must create the VPN tunnel from the user's computer.

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

## VPN client system requirements and limitations

**Table 5.4: VPN Client System Requirements and Limitations**

| Platform | PPTP                                                                                                                                                                                                                                                                                                                                                                                                                    | IPSec                                                                                                                                                                                                                                                                                                                                                |
|----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Windows  | <ul style="list-style-type: none"> <li>Windows XP</li> <li>Windows 2000</li> <li>Windows NT</li> <li>Windows ME</li> <li>Windows 98</li> <li>Windows 95 with DUN1.3 update</li> </ul> Supported authentication method: MS-CHAPv2<br><b>NOTE:</b> 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+. | <ul style="list-style-type: none"> <li>Windows XP</li> <li>Windows 2000</li> </ul> Supported authentication types: <ul style="list-style-type: none"> <li>X.509 certificates (which require the administrator to manually create the certificate files in /etc)</li> <li>RSA public key</li> <li>Preshared key (PSK) requires a static IP</li> </ul> |
| Linux    | PPTP client (pptp-linux)                                                                                                                                                                                                                                                                                                                                                                                                | OpenSWAN                                                                                                                                                                                                                                                                                                                                             |
| MacOS X  | Internet Connect application                                                                                                                                                                                                                                                                                                                                                                                            | MacOS X 10.2 or later                                                                                                                                                                                                                                                                                                                                |

## IPSec VPN connections

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

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 5.5: IPSec VPN Configuration Information for Administrators and Users**

| Value Name              | Description                                                                                |
|-------------------------|--------------------------------------------------------------------------------------------|
| Connection Name         | Any descriptive name you choose.                                                           |
| Authentication protocol | <ul style="list-style-type: none"> <li>AH.</li> <li>ESP.</li> </ul>                        |
| Authentication method   | <ul style="list-style-type: none"> <li>RSA public keys.</li> <li>Shared secret.</li> </ul> |

**Table 5.5: IPSec VPN Configuration Information for Administrators and Users (Continued)**

| Value Name     | Description                                                                                                                                                                                                                                                                                                              |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Boot action    | <ul style="list-style-type: none"> <li>• Ignore.</li> <li>• Add.</li> <li>• Start.</li> <li>• Add and route.</li> </ul>                                                                                                                                                                                                  |
| Remote (Right) |                                                                                                                                                                                                                                                                                                                          |
| ID             | @workstation_name.                                                                                                                                                                                                                                                                                                       |
| IP address     | IP address of the user's workstation.                                                                                                                                                                                                                                                                                    |
| Next hop       | Leave blank if the user's workstation and the OnBoard appliance 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 appliance 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 appliance 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         | Network IP address and netmask for the private subnet where the devices reside that are going to be accessed through the OnBoard appliance.                                                                                                                                                                              |
| 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 appliance.                                                                                                                                                                                  |

The OnBoard appliance administrator must do the following tasks:

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

The OnBoard appliance 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 appliance administrator to create an IPSec VPN connection profile on the user's workstation.

If the OnBoard appliance administrator sends the relevant portions of the `ipsec.conf` file from the OnBoard appliance'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 appliance 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 appliance, using the OnBoard appliance-side IP address assigned to the OnBoard appliance. Use the OnBoard appliance-side IP address configured when the private subnet or virtual network to which the tunnel is connected was being configured.
- Through the OnBoard appliance, enable native IP access to the device.

## PPTP VPN connections

For an authorized user to access native IP functionality on a connected SP, the user needs to create a VPN connection to the OnBoard appliance. 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 appliance administrator before any user can make a PPTP VPN connection:

- Create a VPN connection profile on the OnBoard appliance specifying a pool of addresses for the OnBoard appliance 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 appliance.
- 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 appliance by entering the OnBoard appliance'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 appliance administrator:
  - PPTP server address = OnBoard appliance public IP address (203.1.2.3)
  - Username = OnBoard appliance username
  - 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 appliance's end of the PPTP link.
- Enter the OnBoard appliance's PPTP-assigned address either in a browser or with `ssh` on the command line to access the OnBoard appliance.
- 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 appliance'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.

---

## Configuring Dial-ins Using `cycli`

The following procedures give examples for configuring the two following types of devices for dial-ins.

- An external modem connected to an AUX port
- A modem, GSM or CDMA PCMCIA card installed in one of the PCMCIA slots. Configure the card in slot 1 as `modem0` and configure the card in slot 2 as `modem1`.

See Table 4.16 on page 43 for the values you need to configure for each access type.

**To configure an external modem or a modem, GSM or CDMA PCMCIA card using `cycli`:**

1. Log into the OnBoard appliance console as root.
2. Enter the `cycli` command.

3. If you are configuring an external modem, set the auxport profile to modem.

```
cli> set auxport profile modem OK
```

4. Set the access type to autopp, login, ppp or otplogin.

The following example sets the access type of an external modem to ppp.

```
cli> set auxport modem type ppp
OK
```

The following example sets the access type of a card in slot 1 to ppp.

```
cli> set cards modem0 autopp
OK
```

5. Set or accept the default speed.

The default speed is 9600. The following example sets the external modem speed to 4800.

```
cli> set auxport modem speed 4800
OK
```

The following example sets a modem or phone cards's speed to 4800.

```
cli> set auxport modem speed 4800
OK
```

6. Set or accept the default flow control (data-flow) option.

The following example sets an external modem's data-flow type to both.

```
cli> set auxport modem data-flow both
OK
```

The following example sets a modem or phone card's data-flow type to both.

```
cli> set cards modem0 data-flow both
OK
```

7. Set the chat initialization AT commands (initchat).

Put quotation marks before and after the chat string and put backslashes (\) before any quotation marks or backslashes that are part of the chat string. The examples set the chat string to: initchat " " " ATZ OK.

The following example sets an external modem's chat string.

```
cli> set auxport modem initchat "\"\" ATZ OK"
```

The following example sets a modem or phone card's chat string.

```
cli> set cards modem0 initchat "\"\" ATZ OK"
OK
```

8. If you set the access type to ppp or autopp, set all ppp parameters by performing the following steps.
  - a. Enable authentication as a requirement for PPP connections, if desired, by using the auth parameter followed by yes.

The following example enables authentication for an external modem.

```
cli> set auxport modem ppp auth yes
OK
```

The following example enables authentication for a modem or phone card.

```
cli> set cards modem0 ppp auth yes
OK
```

- b. Accept the default local IP address or set another by using the iplocal parameter.

The following example configures a local IP address for an external modem.

```
cli> set auxport modem ppp iplocal local_ip_address
OK
```

The following example configures a local IP address for a modem or phone card.

```
cli> set cards modem0 ppp iplocal local_ip_address
OK
```

- c. Accept the default remote IP address or set another by using the ipremote parameter.

The following example configures a remote IP address for an external modem.

```
cli> set auxport modem ppp ipremote remote_ip_address
OK
```



The following example configures a remote IP address for a modem or phone PCMCIA card.

```
cli> set cards modem0 ppp ipremote remote_ip_address
OK
```

9. Accept the default maximum transmission unit or set another by using the mtu parameter.

The following example sets the MTU to 1200 for an external modem

```
cli> set auxport modem ppp mtu 1200
OK
```

The following example sets the MTU to 1200 for a modem or phone PCMCIA card.

```
cli> set cards modem0 ppp mtu 1200
OK
```

10. Accept the default maximum receive unit or set another by using the mru parameter.

The following example sets the MRU to 1200 for an external modem

```
cli> set auxport modem ppp mru 1200
OK
```

The following example sets the MRU to 1200 for a modem or phone PCMCIA card.

```
cli> set cards modem0 ppp mru 1200
OK
```

11. Accept the default PPP options or set others by using the options parameter followed by the desired options in quotes.

The following example sets the ppp options for an external modem

```
cli> set auxport modem ppp options "options"
OK
```

The following example sets the ppp options for a modem or phone PCMCIA card.

```
cli> set cards modem0 ppp options "options"
OK
```

12. If configuring a GSM card, set a pin number.

```
cli> set cards gsm pin pin_number
OK
```

13. Commit the changes and quit.

```
cli> commit
OK
cli> quit
```

## Configuring the User's Console Login Menu

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 appliance's console.

The OnBoard appliance administrator can configure the `rmenush` menu to display other options including links to additional submenus or commands by modifying the `/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 appliance 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.
- An 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.

**To modify the user shell menu:**

See *Configuring the User's Console Login Menu* on page 78 for background information and examples.

---

**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. Log into the OnBoard appliance console as root.
2. Open the `/etc/menu.ini` file for editing.
3. Add new menus and menu items as desired, using underscores (`_`) to indicate spaces between words.
  - a. In the `[main]` menu definition, insert a definition for an action or an option for a submenu, as desired.

The following example shows a new menu option with a command defined along with a link to a new submenu identified with the `newsubmenu` keyword.

```
[main]
 Access_Servers = /bin/onbdshell
 Change_Password = /usr/bin/passwd
 New_Menu_Option = command_pathname_and_options
 New_Submenu = newsubmenu
```

- b. Add a definition for a submenu using the defined keyword.

```
[newsubmenu]
 Submenu_Option1 = command_pathname_and_options
 Submenu_Option2 = command_pathname_and_options
```

4. Save and quit the file.

## Configuring Routes With `cycli`

The following procedures give examples for using the `cycli` utility for configuring default, host and network routes and assigning them to interfaces or to gateways.

---

**NOTE:** Setting a gateway IP address automatically creates a default route to the gateway's IP address.

---

**To configure routes with `cycli`:**

1. Log into the OnBoard appliance console as root.
2. Enter the `cycli` command.

3. Make sure the interface for which you want to configure a route is active.

```
cli> set network interface interface_name active
yes
OK
```

4. Set a default route by setting a gateway IP address.

```
cli> set network interface interface_name gateway gatewayIP
OK
```

5. Add a host route, if desired, by entering the host's IP address after the add network `st_routes` command.

```
cli> add network st_routes hostIP
```

6. Add a network route, if desired, by entering the network address after the add network `st_routes` command in the form `1.2.3.4/24`.

```
cli> add network st_routes networkIP/24
OK
```

7. For both host and network routes, use the `set network st_routes` command to assign the route to an interface or to a gateway and optionally assign it a metric, by performing the following steps.

- a. To assign the route to an interface, enter `set network st_routes IPaddress | networkIPaddress/NN device ethN`.

The following screen example shows assigning the host route created in step 5 to the device `eth0` and assigning an optional metric.

```
cli> set network st_routes IPaddress | networkIPaddress/NN ethN \
metric N
OK
```

- b. To assign the route to a gateway, enter `set network st_routes IPaddress | networkIPaddress/NN gateway gatewayIP`.

The following screen example shows assigning the network route created in step 6 to the gateway `192.168.2.0`.

```
cli> set network st_routes IPaddress | networkIPaddress/NN \
gateway gatewayIP
OK
```

## Saving Configuration Changes

As described in *How Configuration Changes Are Handled* on page 55, the Web Manager and the `cycli` utility do not save changes as they are made. The following procedures show the steps administrators need to take to save changes to configuration files in different environments on the OnBoard appliance.

When changes are made by an administrative user using the Web Manager, an **Unsaved changes** button displays until the administrative user clicks the *Save and apply changes* button.

When changes made by the administrator using the `cycli` utility are not saved (committed) and the administrator enters the quit command, the utility displays the prompts shown in the following screen example.

```
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!".
```

### To save configuration changes:

1. If you are logged into the Web Manager as an administrative user, click *Save and apply changes*.
2. To save configuration changes made while using the `cycli` utility, either invoke the **`cycli`** utility using the `-C` option or enter the **`commit`** command after performing configuration and before quitting `cycli`.

## Backing Up Configuration Files

OnBoard appliance administrators can create a compressed backup of all configuration files and store the backup in `/mnt/hda3/backup/configuration_files.gz`. Any compressed configuration file that already resides in the directory is overwritten. The following procedures show how administrators can back up configuration files in different environments on the OnBoard appliance.

### To back up configuration files:

1. If you are logged into the Web Manager as an administrative user, go to the `Mgmt-Backup/restore` screen and click the *Save* button.
2. If you are logged into the OnBoard appliance console as root, enter the **`saveconf`** command.

```
[root@OnBoard root]# saveconf
```

## Restoring Backed Up Configuration Files

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.

**To restore the OnBoard appliance configuration files to the last saved version:**

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 appliance console as root, enter the **restoreconf** command.

```
[root@OnBoard root]# restoreconf
```

## Restoring Factory Default Configuration Files

A root user can restore the factory default configuration files from the `factory_default_files.gz` file by performing the following procedure while logged in through the console, via telnet or ssh to restore the configuration files to the state they were in when the OnBoard appliance shipped. For how to restore factory defaults while you are saving a boot image from RAM memory onto the resident Flash memory, see *To upgrade to a boot image from a network boot in U-boot monitor mode*: on page 277.

**To restore the factory default configuration files from the command line:**

1. Log into the OnBoard appliance console as root.
2. Enter the **restoreconf** command with the `factory_default` option.

```
[root@OnBoard root]# restoreconf factory_default
```

## Adding New 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 an application or a script or a data file 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 appliance console 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.

## Changing Web Manager Time-outs

The OnBoard appliance administrator can log into the console as root and manually change the time-out value for Web Manager logins by editing a configuration file. The default time-out value is 1800 seconds (30 minutes). The value can be changed to any number of seconds up to  $2^{13}$ .

### To configure Web Manager time-outs:

1. Log into the OnBoard appliance console as root.
2. Change to the `/etc/cacpd` directory and open the `cacpd.conf` file for editing.
3. Find the following lines that define the time-out:

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

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

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

## Changing the Sort Order of Device Listings

The names of devices are listed in the Web Manager and by `onbdshell` in the order in which they were configured. An OnBoard administrator can configure device lists to appear in alphabetical order using the `cycli` utility.

### To sort the device list alphabetically:

1. Log into the OnBoard appliance console as an administrative or root user.

```
OnBoard login: root
Password: password
```

2. Enter the **cycli** command.

```
[root@OnBoard root]# cycli
```

3. Set the sort order by entering the onboard global sort server alpha parameters.

```
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 Groups for Use with Authentication Servers

This information applies when an authentication method that relies on an authentication server is configured either for the OnBoard appliance or for a connected device. If the administrator of an authentication server configures users as members of groups as described in this section, the users do not need accounts configured on the OnBoard appliance.

For example, if user johnb is defined as a member of the admin group on a TACACS+ server, johnb can log into the OnBoard appliance as an administrative user when TACACS+ authentication is configured for the appliance, even though no user account is configured for johnb on the OnBoard appliance.

To support the use of groups with the authentication methods that support groups, the administrator must configure local groups on the OnBoard appliance using the same group names used on the authentication servers, using the Web Manager or the cycli utility.

The admin group exists by default. User accounts do not need to be configured on the OnBoard appliance for the users in the authentication-server-defined groups.

## Configuring group authorization for LDAP authentication

LDAP authentication can be provided by either a Windows Active Directory server or a server running OpenLDAP.

### Configuring group authorizations on an Active Directory server

Perform the following procedures for configuring group authorization when a Windows Active Directory server is used for LDAP authentication.

#### To install Windows Administration Pack tools and configure the snap-in:

1. On the server, install the tools from the Windows Administration Pack. The tools are found on the Windows server installation CD.



2. Go the start menu and click *Run*.
3. In the Open field, type **mmc /a** and click *OK*. A console window appears.
4. Click *Console* in the console window menu bar and select *Add/Remove Snap-in...* The Add/Remove Snap-in window appears.
5. Click *Add*. The Add Standalone Snap-ins window appears.
6. Select *Active Directory Schema* from the list of snap-ins and click *Add*.
7. Select *ADSI Edit* from the list of snap-ins and click *Add*.
8. Click *Close*.
9. Click *OK* in the Add/Remove Snap-in... window.

**To configure Active Directory schema:**

1. In the server's console window, double click *Active Directory Schema*. The paths *Classes* and *Attributes* appear.
2. Double click *Attributes* and confirm that the info attribute is present.
3. Double click *Classes*, locate the class *Users* and right-click to select *Properties*.
4. Select the *Attributes* tab and click *Add*.
5. Locate info in the attributes list; click *Apply* and then *OK*

**To configure a group in ADSI Edit:**

1. In the server's console window, double click *ADSI Edit*.
2. From the menu, select *Action-Connect to...* The Connection window appears.
3. Accept the defaults and select *OK*.  
The path *Domain NC<domain>.com* appears.
4. Double click *Domain NC<domain>.com*. The expanded path *DC=xxx,DC=xxx,DC=com* appears.
5. Double click *DC=xxx,DC=xxx,DC=com*.  
The expanded class *CN=Builtin, ...* appears.
6. Double click *CN=Users*. The expanded users list appears.
7. Right-click on the name of a user and select *Properties*. The *CN=<username> Properties* window appears.
8. In the *Optional* area under *Select which property to view*: locate and select *comment*.
9. In the *Edit Attribute* field, enter a group or groups in the form *group\_name=<Group1> [,<Group2,>...,<GroupN>]*; then click *OK*.

---

**NOTE:** To configure the user as an administrative user on the OnBoard appliance, add the admin group name to the definition.

---

10. Close or save the windows.

## Defining groups in an info attribute on an LDAP server

The info attribute must be added to the LDAP definition on the authentication server and users must be assigned groups using the info attribute.

### To configure groups on an LDAP authentication server:

1. On the server, add the info attribute into the objectclass posixAccount in the /etc/ldap/schema/nis.schema file.

```
objectclass (1.3.6.1.1.2.0 NAME 'posixAccount' SUP top AUXILIARY DESC
'Abstraction of an account with POSIX attributes' MUST (cn $ uid $
uidNumber $ gidNumber $ homeDirectory) MAY (userPassword $ loginShell
$ gecos $ description $ info))
```

2. Make sure the info attribute exists in the /etc/ldap/schema/cosine.schema file.

```
attributetype (0.9.2342.19200300.100.1.4 NAME 'info'
DESC 'RFC1274: general information'
EQUALITY caseIgnoreMatch
SUBSTR caseIgnoreSubstringsMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{2048})
```

3. Make sure both schema files are listed in slapd.conf:

---

**NOTE:** The slapd.conf file is normally located in: [Redhat] /etc/openldap or [bsd] /usr/local/etc/openldap.

---

```
include /etc/openldap/schema/nis.schema
include /etc/openldap/schema/cosine.schema
```

4. Restart the LDAP service to activate changes.
5. Use the **ldapadd** command or the **ldapmodify** command, assigning groups using the info attribute. For each user, assign any desired groups in an info definition using the following syntax.

```
info: group_name=<Group1>[,<Group2> , . . . ,<GroupN>] ;
```

---

**NOTE:** To give a user administrative access to the OnBoard appliance, add the admin group name to the above definition.

---

## Configuring group authorization for RADIUS authentication

The two tasks listed below must be done to configure groups for RADIUS authentication.

- The RADIUS server's administrator must define the desired groups and assign users to the groups.

See *To configure groups on a RADIUS authentication server:* on page 87.

- The OnBoard appliance's administrator must configure the RADIUS server on the OnBoard appliance.

The following list defines the values to define when configuring a RADIUS authentication server on the OnBoard appliance as shown below.

```
auth1 server[:port] secret [time-out] [retries]
```

```
acct1 server[:port] secret [time-out] [retries]
```

where:

auth1: The first RADIUS authentication server.

acct1: The first RADIUS accounting server.

server: The RADIUS server address.

port: Optional. The default port name is radius and is looked up through /etc/services.

secret: The shared password required for communication between the OnBoard appliance and the RADIUS server.

retries: The number of times each RADIUS server is tried before another is contacted.

time-out: The default is 3 seconds. How long the OnBoard appliance should wait for the RADIUS server's response.

### To configure groups on a RADIUS authentication server:

1. On the server, open the /etc/raddb/users file for editing.
2. Assign groups to a user in the Framed-Filter-Id attribute.
3. Use the format Framed-Filter-Id=:group\_name=<Group1>[,<Group2>,.... <GroupN>];, as shown in the following example.

```
groupuser1
Auth-Type= Local, Password = "xxxx"
Service-Type=Callback-Framed-User,
Callback-Number="305",
Framed-Protocol=PPP,
Framed-Filter-Id=":group_name=<Group1>[,<Group2>, . . . , <GroupN>];",
Fall-Through=No
```

---

**NOTE:** If the Framed-Filter-Id already exists, append the group\_name declaration to the string starting with a colon (:). Make sure a final semi-colon (;) is at the end of the declaration, as shown in the example.

---

4. Save and quit the file.

**To configure a RADIUS authentication server on the OnBoard appliance:**

1. Log into the OnBoard appliance console as root.
2. Open the `/etc/raddb/server` file for editing or create the file.
3. Make an entry for the RADIUS server (auth1), an accounting server (acct1) and if desired, make an entry for a second RADIUS authentication server (auth2) and for a second accounting server (acct2), by performing the following steps for each server.
4. Follow the file configuration directions shown in the following example.

```
For proper security, this file SHOULD have permissions 0600,
that is readable by root, and NO ONE else. If anyone other than
root can read this file, then they can spoof responses from the
server!

#

There are 3 fields per line in this file. There may be multiple
lines. Blank lines or lines beginning with '#' are treated as
comments, and are ignored. The fields are:
#
server[:port] secret [timeout]
#
the port name or number is optional. The default port name is
"radius", and is looked up from /etc/services The timeout field is
optional. The default timeout is 3 seconds.
#
If multiple RADIUS server lines exist, they are tried in order. The
first server to return success or failure causes the module to return
success or failure. Only if a server fails to response is it skipped,
and the next server in turn is used.
#
The timeout field controls how many seconds the module waits before
deciding that the server has failed to respond.
#
server[:port] shared_secret timeout (s)
127.0.0.1 secret 1
other-server other-secret 3

OUR.RADIUS.SERVER.IP:1645 OurSecret 1 3
```

5. Enter the IP address for the server.
6. Optional: define an alternate port.
7. Enter the secret (shared password).
8. Optional: enter a value to redefine the time-out.
9. Optional: enter a value to redefine the number of retries.

The following screen example shows entries that define the RADIUS authentication server and the accounting server to be the same server with the same IP address, sets the secret to cyclades, the time-out to 5 seconds and the number of retries to 5.

```
auth1 172.20.0.2 cyclades 5 5
acct1 172.20.0.2 cyclades 5 5
```

---

**NOTE:** Always configure both parameters auth1 and acct1.

---

10. Save and quit the file.

---

**NOTE:** Multiple RADIUS servers can be configured in this file. The servers are tried in the order in which they appear. If a server fails to respond, the next configured server is tried.

---

## Configuring group authorization for TACACS+ authentication

The two tasks listed below must be done to configure groups for TACACS+ authentication.

- The TACACS+ server's administrator must define the desired groups and assign users to the groups.
- The OnBoard appliance's administrator must configure the TACACS+ server on the OnBoard appliance. The administrator of the OnBoard appliance, must configure the TACACS+ authentication server for raw access. Table 5.6 lists two ways to perform the needed configuration.

**Table 5.6: Methods for Configuring the TACACS+ Authentication Server for Raw Access**

| Method                         | Where Documented                                                                                                                                      |
|--------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| Web Manager                    | <i>To configure a TACACS+ authentication server:</i> on page 151<br><b>NOTE:</b> Make sure to check the <i>Enable Raccess Authorization</i> checkbox. |
| OnBoard appliance command line | <i>Configuring a TACACS+ authentication server on the OnBoard appliance</i> on page 90                                                                |

The following cycli utility command line can also be used to configure a server for raw access:

```
cli> set auth tacplus service raccess
```

**To assign a group to a user on the TACACS+ server:**

1. Add a definition for the group to the authentication authorization accounting (AAA) database on the TACACS+ server.

---

**NOTE:** These additions can be made through a GUI. The example shows the configuration if a GUI is not available.

---

```
#####
Group Definitions
#####
group = group_name {
 ...
}
```

2. To the definition for each user, add the raccess service in the form service = raccess and assign the desired group to the user in the form member = group\_name.

---

**NOTE:** Each user may belong to only one group. To give a user administrative access to the OnBoard appliance, assign the admin group.

---

```
#####
User Definitions
#####
user = username {
 service = raccess
 member = group_name
}
```

**Configuring a TACACS+ authentication server on the OnBoard appliance**

The following list defines the values that must be defined in the OnBoard appliance's /etc/tacplus.conf file.

- authhost1: IP address of the TACACS+ authentication server. A second TACACS+ authentication server can be configured with the parameter authhost2.
- accthost1: IP address of a TACACS+ accounting server, which can be used to track how long users are connected after being authorized by the authentication server. Its use is optional. If this parameter is not defined, accounting is not performed. If the same server is used for authentication and accounting, both parameters must be defined with the same address. A second TACACS+ accounting server can be configured with the parameter accthost2.
- secret: The shared secret (password) necessary for communication between the OnBoard appliance and the TACACS+ servers.

- **encrypt:** The default is 1, enable encryption. A value of 0 means disable encryption.
- **service:** The service to be enabled, in this case: raccess.
- **protocol:** The default is lcp (line control protocol). Specify another parameter if required.
- **timeout:** The time-out (in seconds) for a TACACS+ authentication query to be answered.
- **retries:** Defines the number of times a TACACS+ server is tried before another is contacted. The first server authhost1 is tried for the specified number of times, before the second authhost2, if configured, is contacted and tried for the specified number of times. If the second server fails to respond or if no second server is configured, TACACS+ authentication fails.

**To configure a TACACS+ authentication server on the OnBoard appliance:**

1. Log into the OnBoard appliance console as root.
1. Open the `/etc/tacplus.conf` file for editing.
2. Change the values described under *Configuring a TACACS+ authentication server on the OnBoard appliance* on page 90.

---

**NOTE:** To configure group access on the TACACS+ authentication server, service must be defined as raccess.

---

3. Save and quit the file.





## Using the Web Manager

### Logging Into the Web Manager for Administrative Users

Two types of administrative users can access all the Web Manager functions:

- An administrator who knows the password for the admin account, which is configured by default
- An optionally-added administrative user (a regular user whose account is in the admin group)

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. Also like regular users, administrative users can use default menu options that appear on the first Web Manager screen after login to access devices, manage power and change their own passwords.

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 appliance features that enable the enforcement of the organization's security policies. Only one administrative user can connect to the Web Manager at a time. A message appears if another administrative user is currently logged in and provides the option either to cancel the login attempt or to log out the currently-logged-in administrative user.

---

**NOTE:** For security, a login session terminates after a defined period of inactivity. An OnBoard appliance administrator can change the time-out value as described in *Changing Web Manager Time-outs* on page 83.

---

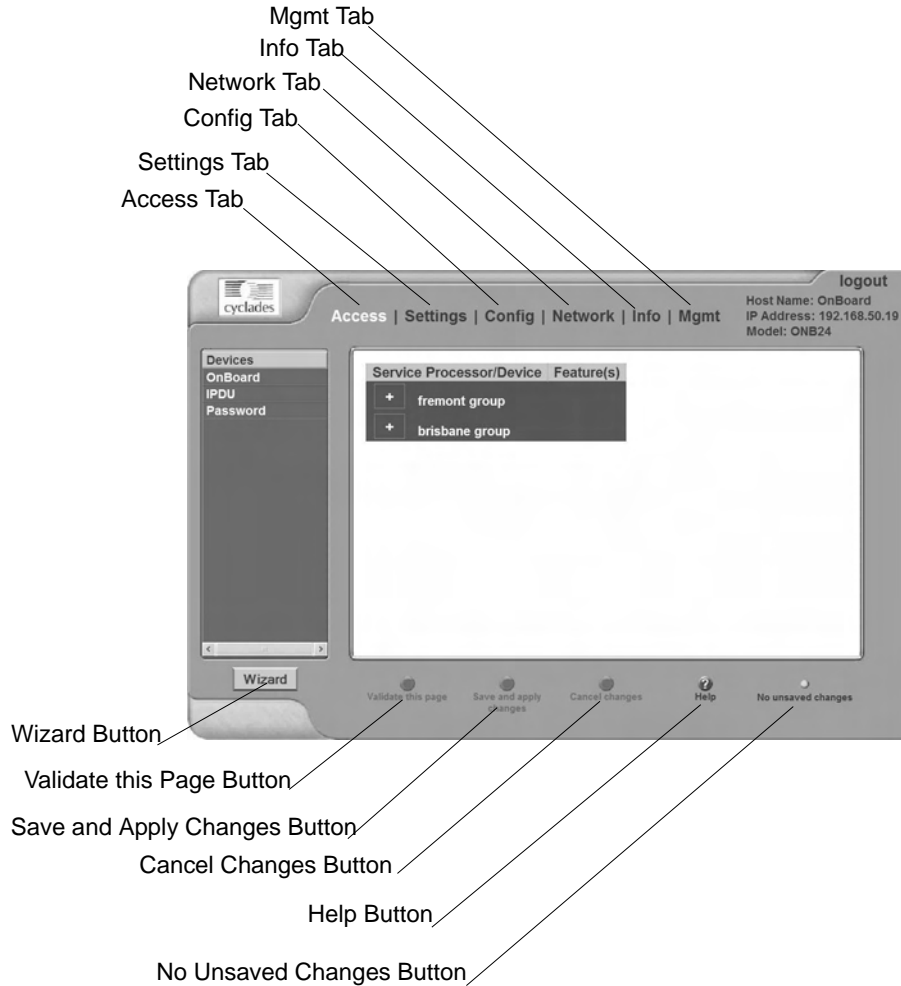
#### To log into the Web Manager as an administrative user:

This procedure assumes you know the password for the admin account or the username and password for an administrative user account and that you have either a network connection or a dial-in connection over a phone line.

1. Enter the IP address of the OnBoard appliance in a supported browser. The Web Manager login screen appears.
2. Enter the username and password.
3. Click the *Login* button.

## Features of administrative users' screens

Callouts in the following figure indicate unique features of the Web Manager that appear when an administrative user logs in.



**Figure 6.1: 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 Figure 6.1) often has several related screens associated with it. The related screens are accessed as tabs.

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 6.2: Example Dialog: Devices Configuration in Wizard Mode

## Web Manager Wizard

How administrative users use the Web Manager Wizard is described in the following sections.

## Using the Wizard

The Wizard screen displays a list of options in the left menu, as shown in Figure 6.3. An administrative user can use the menu options to perform basic configuration of the OnBoard appliance.

**Highlighted Menu Option**

**Next Button**



**Cancel Wizard Button**

**Figure 6.3: OnBoard Appliance Configuration Wizard Screen**

The *Cancel Wizard* button 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 6.4) 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 box appears with a warning.

After the *Next* button is clicked on the last screen of the Wizard, the screen shown in Figure 6.4 appears. Clicking the *Next* button on this screen saves all changes made on any of the Wizard screens.



Figure 6.4: Wizard Confirm Changes Screen

## Changing the administrative user's password

Figure 6.5 shows the screen that appears when the Administrator password option is selected from the Wizard menu.



Figure 6.5: 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:

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

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 *OnBoard Appliance Security Profiles* on page 30.

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. For more details, see *OnBoard Appliance Services* on page 32.

Clicking the Proceed button on the Security Profile Caution screen brings up the Security Profile configuration dialog. An administrative user can use the dialog to select one of the default security profiles or configure a custom security profile.

The Moderate profile is the default option selected on the Security level menu. See Chapter 4 for more information on security profiles.

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.

---

**NOTE:** If you select the secured profile, follow the reminder at the bottom of the screen 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.

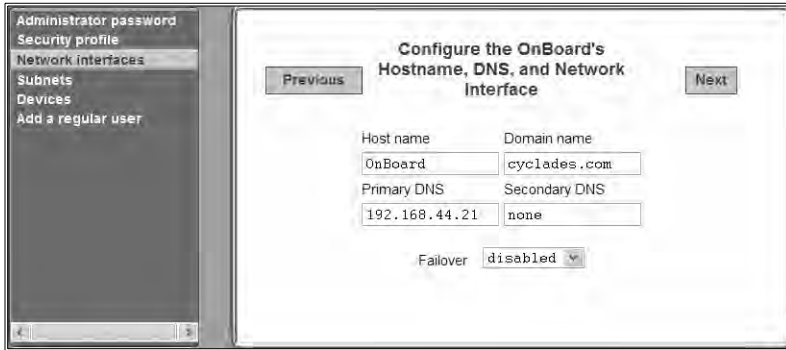
---

### To select or configure a security profile:

1. Log into the Web Manager as an administrative user.
2. Click the *Wizard* button.
3. Click the Security profile option in the left menu bar.
4. Click the *Proceed* button.
5. Select a security profile from the Security Level pull-down menu.
6. 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.
7. Click *OK*. The security profile confirmation screen appears.
8. Click *Save and apply changes*.
9. Click *Next*, if desired, to go to the next Wizard screen.

## Configuring network interfaces

Figure 6.6 shows the first of a series of related screens that appears when the Network interfaces option is selected from the Wizard menu.



**Figure 6.6: Network Interfaces Screen**

The screen shown in Figure 6.6 allows the administrative user to set or change the parameters in the following table.

**Table 6.1: 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 appliance                                                                                                                                                         |
| Secondary DNS server | IP address for an optional secondary DNS server on the same subnet as the OnBoard appliance                                                                                                                                             |
| 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 <i>Ethernet Ports on the OnBoard Appliance</i> 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 100 and *Configuring primary and secondary Ethernet ports* on page 101.

Table 6.2 describes the parameters that can be set on the failover configuration screen and on the primary and secondary Ethernet configuration screens.

**Table 6.2: Ethernet Port Settings**

| Settings     | Notes                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|--------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DHCP         | DHCP is enabled by default on the OnBoard appliance's interfaces. If DHCP is enabled, the OnBoard appliance looks for a DHCP server on the same network. If a DHCP server cannot be located, the OnBoard appliance 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 appliance                                                                                                                                                                                                                                                                                                                                                                                  |
| MTU          | The maximum transmission unit value for the Ethernet port. Default=1500.                                                                                                                                                                                                                                                                                                                                                                              |
| Broadcast IP | The reserved broadcast IP address.                                                                                                                                                                                                                                                                                                                                                                                                                    |

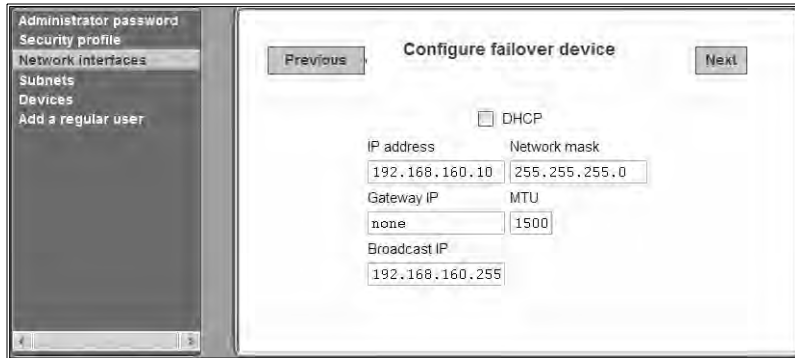
### Configuring routes

Configuring the network interfaces sets up a default route for the OnBoard appliance. When the *DHCP* checkbox is checked on any of the network interface screens, the DHCP server assigns the OnBoard appliance 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. Figure 6.7 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 6.7: 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 6.7 apply to the single bond0 interface.

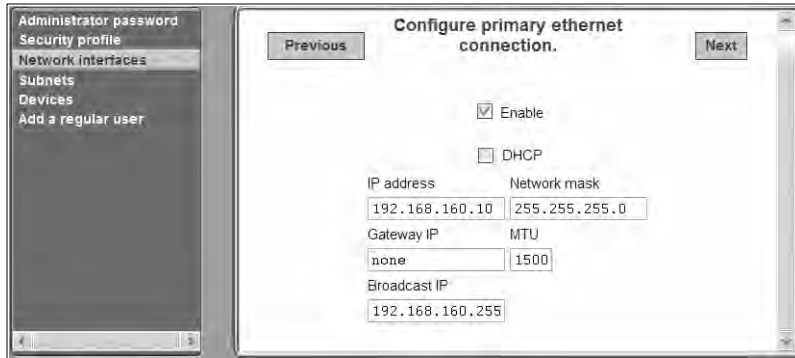
### Configuring primary and secondary Ethernet ports

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.

Figure 6.8 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 appliance to use a static IP address.



**Figure 6.8: 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 appliance network interfaces:**

1. Log into the Web Manager as an administrative user.
2. Click the *Wizard* button.
3. Click the *Network interfaces* option in the left menu bar.
4. Modify the name in the Host name field, if desired.
5. Enter or modify an existing DNS domainname in the Domain name field.
6. Enter or modify the IP address for a primary DNS server into the Primary DNS field.
7. Enter or modify the IP address for a secondary DNS server in the Secondary DNS field.
8. Enable or disable failover by selecting the desired option from the Failover pull-down menu.
9. 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.

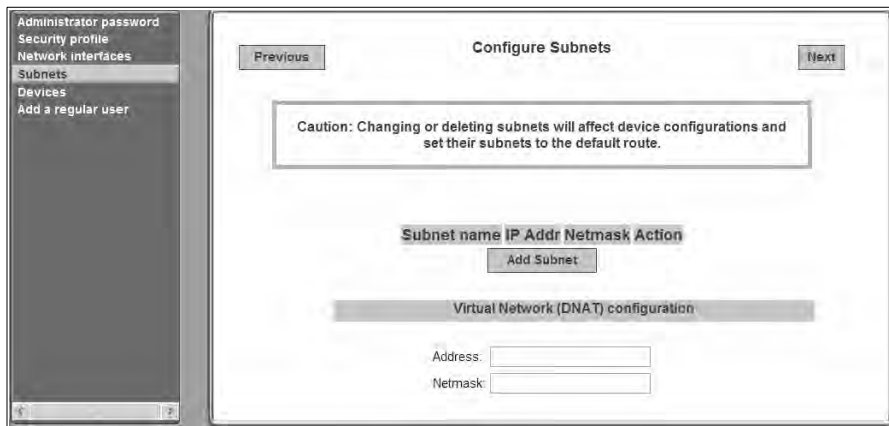
---

- If failover is enabled, clicking the *Next* button brings up a screen for configuring the failover device.
10. If desired, enable DHCP on any of the network interface configuration screens, by clicking the *DHCP* checkbox.
  11. 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.
12. 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.
  13. Click *Save and apply changes*.
  14. Click *Next*, if desired, to go to the next Wizard screen.

## Configuring private subnets and virtual addresses

Figure 6.9 shows the Configure subnets screen that appears when the administrative user selects the Subnets option from the Wizard menu.



**Figure 6.9: Configure Subnets Screen**

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

## Configuring private subnets

Clicking the *Add Subnet* button on the Configure Subnets screen brings up the Private Subnet configuration dialog. At least one private subnet must be defined to enable devices that are connected to the OnBoard appliance's private Ethernet ports to communicate over the Internet via the OnBoard appliance's public IP address. Any number of private subnets may be configured.

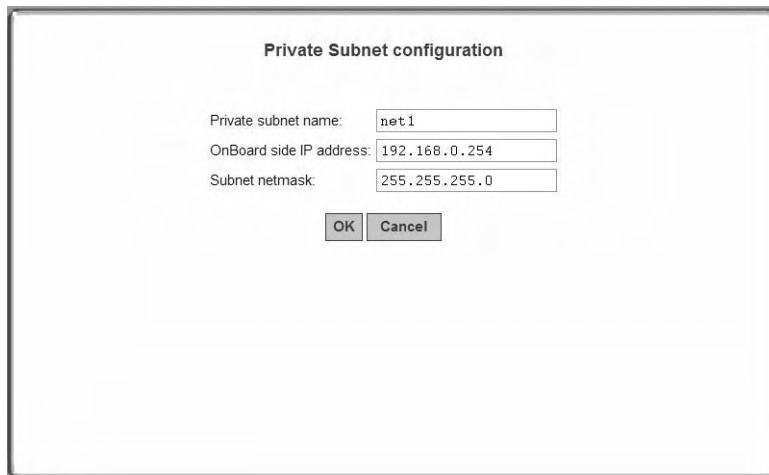
The following table defines the information that the administrative user must supply in the fields that define a subnet.

**Table 6.3: 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 appliance. The OnBoard appliance 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 appliance derives the range of addresses in the subnet from the OnBoard appliance-side IP address and the subnet mask. The OnBoard appliance uses the specified information to create a route to the subnet in the OnBoard appliance's routing table.

The example in Figure 6.10 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.



Private Subnet configuration

Private subnet name:

OnBoard side IP address:

Subnet netmask:

**Figure 6.10: 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:**

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

1. Log into the Web Manager as an administrative user.
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 *Next*, if desired, to go to the next Wizard screen.

## **Configuring a virtual network**

A virtual network based on 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 want 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

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

**Table 6.4: Fields on the Private Subnet Virtual Network Configuration Dialog**

| Field   | Description                                                                                                                                                                                                                             |
|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Address | IP address to assign to the OnBoard appliance from the virtual network. 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 for the OnBoard appliance 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 <i>NNN.NNN.NNN.N</i> , as in: 255.255.255.0.                               |

**To configure a private subnet and optional virtual network:**

1. Log into the Web Manager as an administrative user.
2. Click the *Wizard* button.
3. Click the *Subnets* left menu option.
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 *Next*, if desired, to go to the next Wizard screen.

## Configuring devices

Figure 6.11 shows the Configure devices screen that appears when the *Devices* option is selected from the Wizard menu.

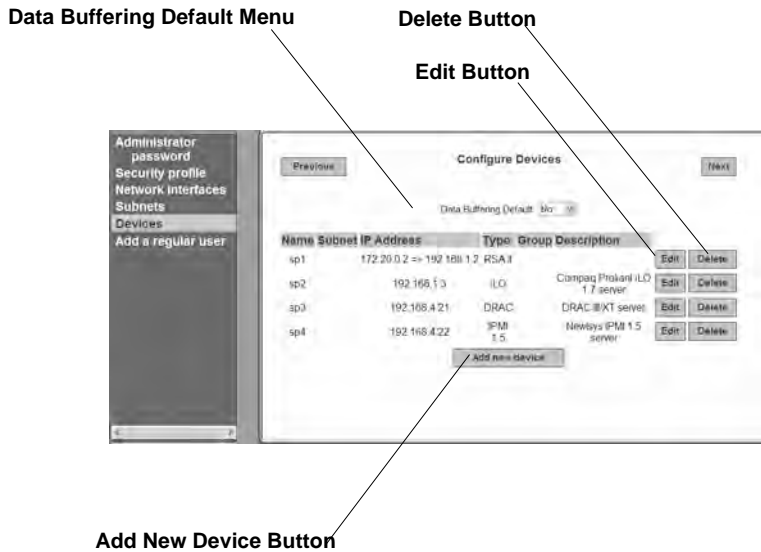


Figure 6.11: Configure Devices Screen

Clicking the *Add new device* button or the *Edit* button next to the entry for an existing device brings up the dialog shown in Figure 6.12.

The dialog box contains the following fields and options:

- Caution:** Setting private subnet to "none" enables the device to be accessed through the public network.
- Name:** [Text input]
- Private subnet:** [Dropdown menu, value: none]
- Login:** [Text input]
- Device IP address:** [Text input]
- Password:** [Text input]
- Virtual IP address:** [Text input]
- Retype password:** [Text input]
- Description:** [Text input]
- Device group:** [Dropdown menu, value: none]
- Authentication type:** [Dropdown menu, value: Local]
- Type:** [Dropdown menu, value: iLO]
- Command template:** [Dropdown menu, value: no template]
- Data buffering:** [Dropdown menu, value: Default]
- Buttons:** OK, Cancel

Figure 6.12: Add New Device and Edit Dialog

**CAUTION:**All devices connected to the private Ethernet ports of the OnBoard appliance must have a previously-configured private subnet name assigned. Otherwise, the device can only be accessed if it is connected to the public interface of the OnBoard appliance, a highly unlikely scenario and one that is not recommended.

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

## Configuring regular users

Figure 6.13 shows the screen that appears when the *Add a regular user* option is selected from the Wizard menu.

**Figure 6.13: Add a Regular User Screen**

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 Figure 6.14.

**Figure 6.14: Fields for Setting a PPP or PPTP Password**

---

**CAUTION:** The caution at the top of the screen shown in Figure 6.13 is a reminder that configuring device management actions for a user gives the user the same device management authorizations for all configured devices. To configure a user 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 create and authorize a user for device management:

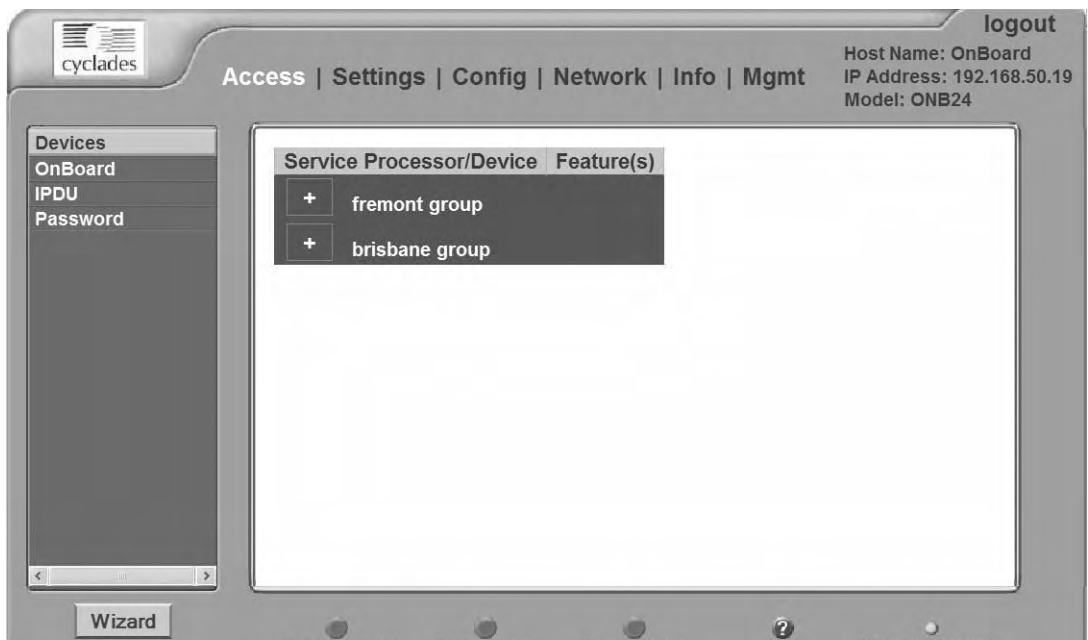
1. Log into the Web Manager as an administrative user.
2. Click the *Wizard* button.
3. Click the *Add a regular user* left menu option.
4. Enter a name in the Username field.
5. Enter identifying (GECOS-type) information in the Full name field.
6. Enter a password in the Password field.
7. Enter the 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.
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 *Next* 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.

## Web Manager Access Menu Options 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 Figure 6.15.



**Figure 6.15: 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.

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

- *Accessing the OnBoard appliance console through the Web Manager*
- *Upgrading IPDU software* on page 111

## Accessing the OnBoard appliance console through the Web Manager

After an administrative user clicks the *Access-OnBoard* menu option, enters the correct password and is authenticated, then the administrative user can do any of the following:

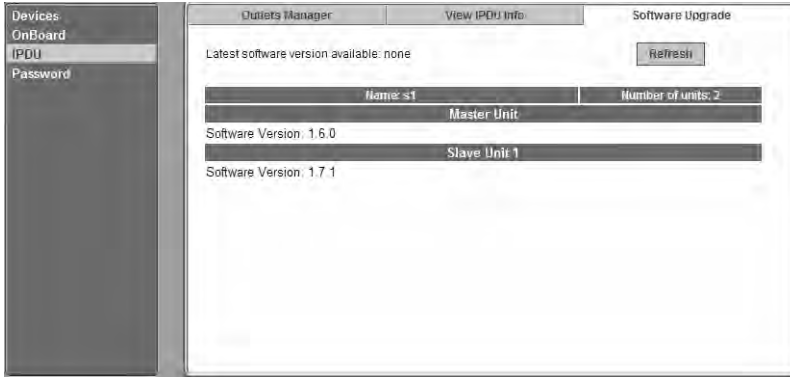
- Access the *cycli* utility to perform command line configuration
- Run the *onbdshell* utility to access devices
- Enter commands that do not require root to succeed
- Run commands that require root to succeed by entering the *sudo* command followed by the name of the command

### To access the OnBoard's console:

1. Bring up the Web Manager and log in as an administrative user.
2. Select the *Access-OnBoard* menu option.
3. If this is the first time you are accessing the OnBoard appliance's console, do the following steps. If this is not the first time you accessed the console, the login prompt for the OnBoard appliance appears. Go to step 4.
  - a. Press **Enter** at the prompt to confirm the saving of the OnBoard appliance's IP address. A dialog asks if you want to add the OnBoard appliance to your set of known hosts.
  - b. Press the *Yes* button. The login prompt for the OnBoard appliance appears.
4. Log into the OnBoard appliance.
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.

## Upgrading IPDU software

To view and upgrade the software on any connected and configured IPDUs, click the *Software Upgrade* tab under the Access-IPDU menu option. Figure 6.16 shows the screen layout that appears.



**Figure 6.16: IPDU Software Upgrade Screen**

A directly-connected IPDU is referred to as the Master Unit and any daisy-chained IPDUs are referred to as Slave 1 through Slave N.

---

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

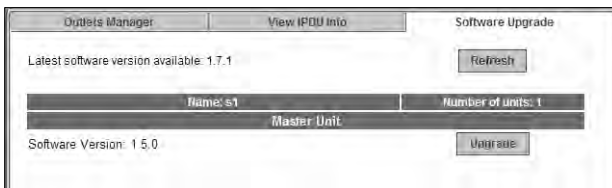
---

Clicking the *Refresh* button has effects shown in Figure 6.17, but only if both the following are true:

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

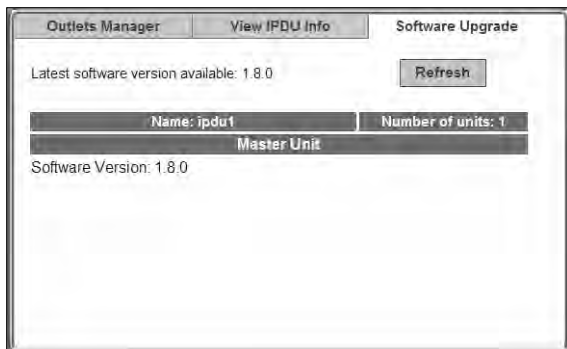
As shown in Figure 6.17, the following appear on the screen if the two prerequisites in the previous list are true:

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



**Figure 6.17: Upgrade Button on the IPDU Software Upgrade Screen**

Pressing the Upgrade button starts the upgrade process. A message displays when the selected IPDU is being upgraded. When upgrading is complete, you are prompted to select *OK*. The Software Upgrade screen then appears and displays the new software version for the selected IPDU.



**Figure 6.18: IPDU Software Upgrade Screen With Upgraded Software**

#### **To download Cyclades PM IPDU software from Cyclades:**

1. Log into the OnBoard appliance's console as an administrative user.
2. Change to the /tmp directory where the software must 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
...
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 than 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 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
...
56916 bytes received in 0.01 secs (7783.5 kB/s)
```

- 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
```

- Log out from the console session and perform the next procedure to update the software.

### To upgrade software on a connected IPDU:

- Make sure that the most recent version of the Cyclades PM IPDU software has been downloaded and copied into the OnBoard appliance's /tmp directory with the filename pmfirmware.
- Log into the Web Manager as an administrative user.
- Select the *Access-IPDU-Software Upgrade* menu option. The Software Upgrade screen displays.
- 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 value next to Latest software version available: changes to match the version in /tmp/pmfirmware, and an Upgrade button appears.
- Click *Upgrade*. A dialog displays while the software is being upgraded.
- When the OK button displays on the dialog, click *OK*.
- Repeat step 5 and step 6 for all listed IPDUs until all are upgraded to the same level.

## Web Manager 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 6.5: Options Under Settings**

| Option             | Where Described                                       |
|--------------------|-------------------------------------------------------|
| AUX port           | <i>Configuring the AUX port</i> on page 115           |
| IPDU               | <i>Configuring IPDU Power Management</i> on page 119  |
| PCMCIA             | <i>Configuring PCMCIA cards</i> on page 123           |
| Date/time          | <i>Configuring system date and time</i> on page 132   |
| Boot configuration | <i>Configuring the boot file location</i> on page 133 |
| Outbound email     | <i>Configuring outbound email</i> on page 135         |

**Table 6.5: Options Under Settings (Continued)**

| Option | Where Described                                                |
|--------|----------------------------------------------------------------|
| Help   | <i>Configuring an alternate help file location on page 136</i> |

## Configuring the AUX port

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 PM IPDUs
- An external modem

### Configuring the AUX port for IPDU power management

Figure 6.19 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 6.19: Settings-AUX Port-Power Management**

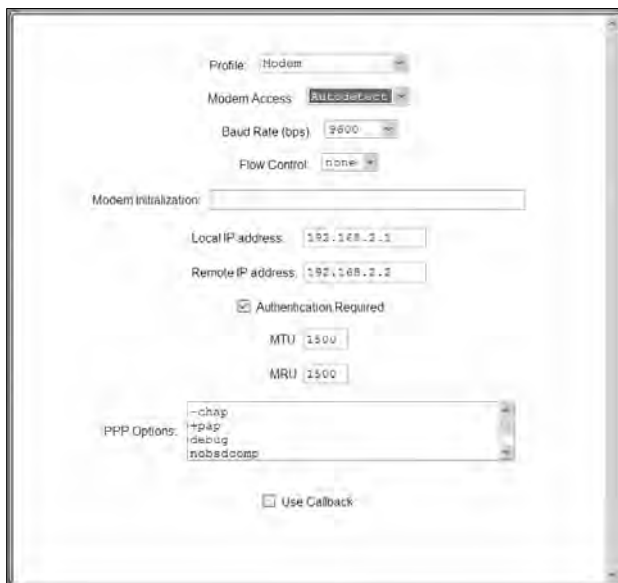
### To configure an AUX port for IPDU power management:

This procedure assumes that a Cyclades PM IPDU is connected to the AUX port of the OnBoard appliance.

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

### Configuring the AUX port for a modem

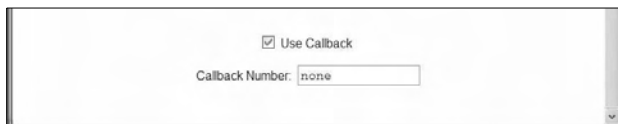
Selecting *Modem* or *GSM* from the Profile pull-down menu on the Settings-AUX port screen causes the fields and menu option shown in the following figure to appear.



**Figure 6.20: Settings-AUX Port -Modem**

An administrative user can use this dialog to configure an external modem connected to the AUX port for dial-in using PPP or login access. The configuration values to select or to enter are described in Table 4.16 on page 43.

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



**Figure 6.21: Callback Number Field Under Settings-AUX Port -Modem**

## Modem access type menu options

If *Autodetect* is selected from the Modem Access pull-down menu, the fields, menus and checkbox shown in Figure 6.20 appear. 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.

If *PPP* is selected from the Modem Access pull-down menu, the field, menus and checkbox shown in the following figure appear.



Profile: Modem

Modem Access: PPP

Baud Rate (bps): 9600

Modem Initialization:

Local IP address: 192.168.2.1

Remote IP address: 192.168.2.2

Authentication Required

MTU: 1500

MRU: 1500

PPP Options: -chap, +pap, debug, nobsdcomp

Use Callback

**Figure 6.22: Settings-AUX Port -Modem -PPP**

If *Login* is selected from the Modem Access pull-down menu, the fields, menu and checkbox shown in Figure 6.23 appear.

Profile: Modem

Modem Access: Login

Baud Rate (bps): 9600

Flow Control: none

Modem Initialization:

Use Callback

**Figure 6.23: Settings-AUX Port -Modem -Login**

If *OTP* is selected from the Access Type pull-down menu, the fields, menu and checkbox shown in Figure 6.24 appear.



**Figure 6.24: Settings-AUX Port-Modem-OTP**

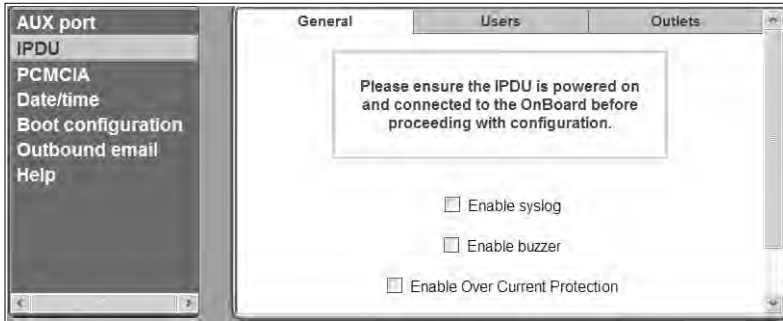
**To configure an AUX port for modem access:**

This procedure assumes that an external modem is connected to the AUX port of the OnBoard appliance. The values to select or to enter for modem configuration are described in Table 4.16 on page 43.

1. Log into the Web Manager as an administrative user.
2. Select the *Settings-AUX Port* menu option.
3. Make sure the *Modem* option is selected from the Profile menu.
4. Choose *Login*, *Autodetect*, *PPP* or *OTP* from the Modem access menu.
5. Select a baud rate from the Baud Rate pull-down menu.
6. If you chose either Login or Autodetect, 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 local IP address or accept the default provided in the Local IP address field.
  - b. Enter a remote 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.
9. Enable callback, if desired, by doing the following steps.
  - a. Check the *Use Callback* checkbox.
  - b. Enter a callback phone number in the Callback Number field.
10. Click *Save and apply changes*.

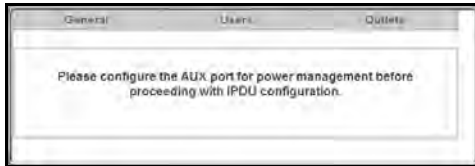
## Configuring IPDU Power Management

When an administrative user clicks the IPDU option under Settings, the following screen appears.



**Figure 6.25: Settings-IPDU Screen**

As shown in Figure 6.25, when the AUX port is configured for power management, three tabs appear for configuring connected IPDU(s). Selecting Settings-*IPDU* without first configuring the AUX port for power management causes the message shown in the following figure to appear.



**Figure 6.26: 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.

---

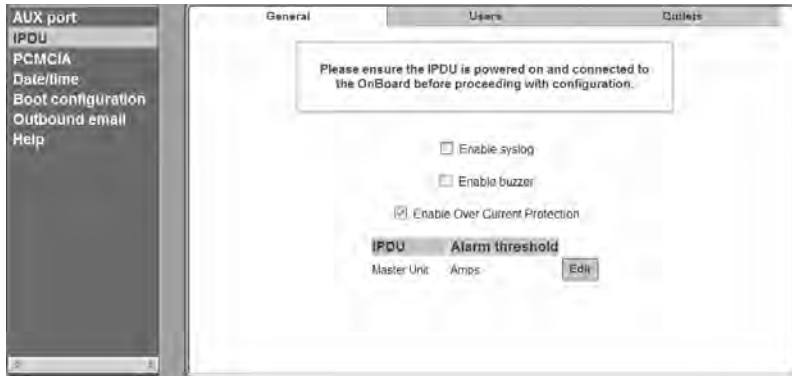
Table 6.6 lists the tabs on the Settings-IPDU screen with links to the sections where they are described.

**Table 6.6: Options Under Settings-IPDU**

| Option  | Where Described                                                                             |
|---------|---------------------------------------------------------------------------------------------|
| General | <i>Configuring over current protection for an IPDU on page 120.</i>                         |
| Users   | <i>Configuring users to manage power outlets on a connected IPDU on page 121.</i>           |
| Outlets | <i>Configuring names and power up intervals for outlets on a connected IPDU on page 122</i> |

## Configuring over current protection for an IPDU

When an administrative user selects the *Settings-IPDU-General* tab, a warning and three options with checkboxes appear, as shown in the following screen example.



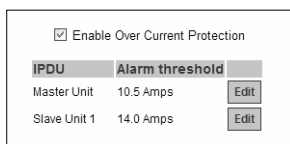
**Figure 6.27: Settings IPDU General Screen**

The settings on the page shown in Figure 6.27 apply to all 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 appliance 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
- Checking *Enable buzzer* causes a buzzer to sound on the IPDU

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 6.28: Settings IPDU General Screen**

Clicking the *Edit* button in the entry for an IPDU brings up the alarm threshold screen. The appropriate value to enter in the Alarm Threshold field varies because each IPDU support a different number of amps. 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 IPDU:

1. Log into the Web Manager as an administrative user.
2. Select the *Settings-IPDU-General* menu option.
3. Check the *Enable Over Current Protection* checkbox, 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 IPDU in the Alarm Threshold field.
  - c. Click *OK*.
4. Check the *Enable syslog* checkbox to enable messages to be sent to the console if the alarm threshold is exceeded.
5. Check the *Enable buzzer* checkbox to cause a buzzer to sound on the PM if the alarm threshold is exceeded.
6. Click *OK*.
7. Click *Save and apply changes*.

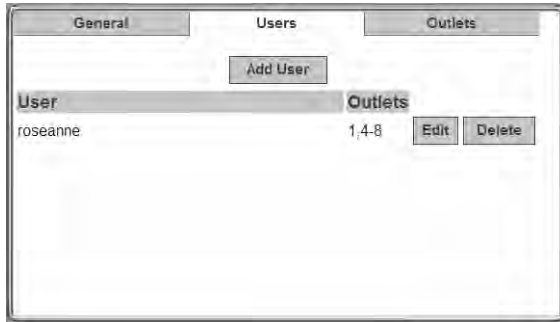
## Configuring users to manage power outlets on a connected IPDU

After selecting the *Settings-IPDU-Users* tab, an administrative user can authorize regular users to manage power outlets. The following figure shows the screen that displays when a single IPDU 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 6.29: 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 usernames and one or more outlets.



**Figure 6.30: Settings-IPDU-Users-Add User Dialog**

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

### **To configure a user to manage power outlets on a connected IPDU:**

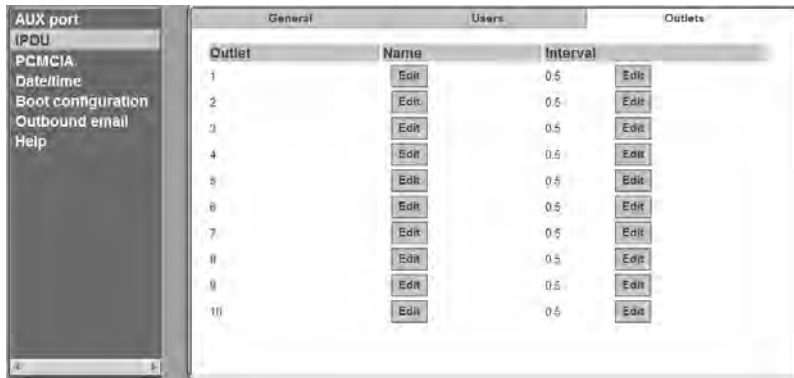
This procedure assumes the following prerequisites:

- An IPDU is connected to the AUX port of the OnBoard appliance. The AUX port is configured for power management.
  - The user account has been defined under *To create and authorize a user for device management*: on page 108.
1. Log into the Web Manager as an administrative user.
  2. Select the *Settings-IPDU-Users* menu option.
  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**

After selecting the *Settings-IPDU-Outlets* tab, 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 6.31: Settings-IPDU-Outlets Screen**

When the Edit button is clicked in the Name column, the outlet name dialog box appears. When the Edit button is clicked in the Interval column, the outlet power up interval dialog box appears.

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. Select the *Settings-IPDU-Outlets* menu option.
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**

If an administrative user selects the *Settings-PCMCIA* menu option, the administrative user can use the PCMCIA screen to insert, eject and configure PCMCIA cards. 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 6.7: PCMCIA Action Buttons**

| Action    | Notes                                                                                  |
|-----------|----------------------------------------------------------------------------------------|
| Insert    | Click this button before physically inserting the card.                                |
| Eject     | Click this button before physically ejecting the card.                                 |
| Configure | Click this button to bring up a dialog for configuring the card according to its type. |

The following procedure describes the configuration steps to begin configuring any PCMCIA card.

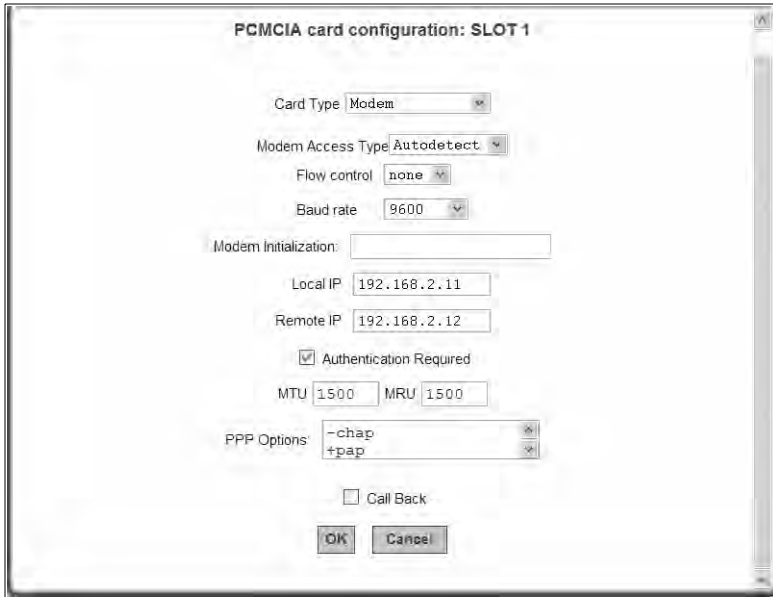
**To begin configuring a PCMCIA card:**

1. Log into the Web Manager as an administrative user.
2. Select the *Settings-PCMCIA* menu option. 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 the card into one of the slots on the front of the OnBoard appliance.
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 the card type to configure from the pull-down menu. The PCMCIA card configuration dialog appears.

**Configuring a modem or GSM the card**

Selecting either *Modem* or *GSM* from the Card Type pull-down menu on the PCMCIA card configuration dialog cause the fields, menu options and checkbox shown in the following figure to appear.





**Figure 6.32: Settings-PCMCIA-Configure Dialog-Modem or GSM**

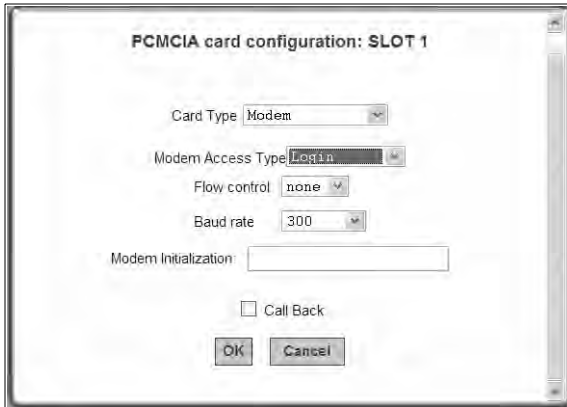
An administrative user can use this dialog to configure an installed modem or GSM PCMCIA card for dial-ins using PPP or login access. The configuration values to select or to enter are described in Table 4.16 on page 43.

If the *Call Back* checkbox is selected, then an additional field for the phone number appears.

### **Access type menu options**

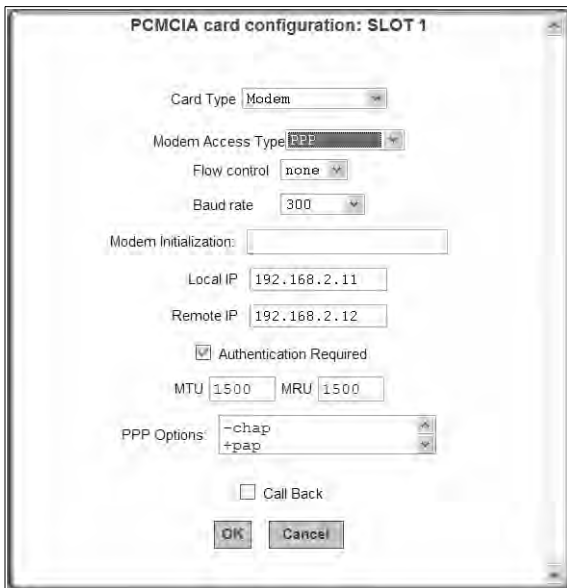
If *Autodetect* is selected from the Access Type pull-down menu, the fields, menus and a checkbox shown in Figure 6.33 appear. Because autodetection can detect either a PPP or Login access attempt, the screen has fields and pull-down menus for configuring all the parameters that apply to both options.

If *Login* is selected from either the Modem Access Type, the GSM Access Type or CDMA Access Type pull-down menu, the fields, menu and checkbox shown in the following figure appear.



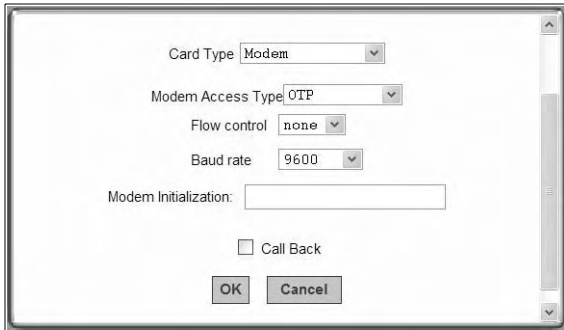
**Figure 6.33: Settings-PCMCIA-Configure Modem or GSM-> Login**

If *PPP* is selected from the Access Type pull-down menu, the fields, the menu and the checkbox shown in the following figure appear.



**Figure 6.34: Settings-PCMCIA-Configure Modem or GSM-PPP**

If *OTP* is selected from the Access Type pull-down menu, the fields, the menu and the checkbox shown in the following figure appear.



**Figure 6.35: Settings-PCMCIA-Configure Modem or GSM-OTP**

---

**NOTE:** Configuration of OTP authentication through the Web Manager is only supported for modem or GSM cards.

---

### To configure a modem or GSM PCMCIA card:

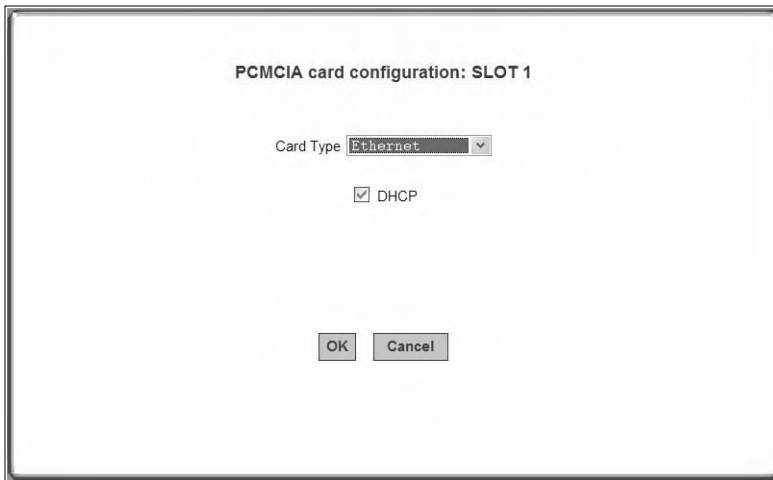
This procedure assumes that a modem or GSM PCMCIA card is inserted into a slot on the OnBoard appliance and the steps under *To begin configuring a PCMCIA card:* on page 124 are complete. See Table 4.16 on page 43 for the values that an administrative user needs to select or to enter for modem configuration, if needed.

1. Log into the Web Manager as an administrative user.
2. Select the *Settings-PCMCIA* menu option.
3. Make sure that *Modem* or *GSM* is selected from the Card Type pull-down menu on the PCMCIA card configuration dialog.
4. Select either *Login*, *Autodetect*, *PPP* or *OTP* from the Modem Access Type pull-down menu.
5. Select an option from the Flow control pull-down menu.
6. Select a baud rate from the Baud rate pull-down menu.
7. Enter a modem chat string in the Modem Initialization field.
8. To enable callback, do the following steps.
  - a. Check the *Call Back* checkbox. The Phone Number field appears on the Slot dialog box.
  - b. Enter a number for the OnBoard appliance to use when calling back the remote user's modem or phone.
9. 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.
  - b. Enter a remote 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. Enter PPP options as desired in the PPP Options field.
10. Enable callback, if desired, by doing the following steps.
    - a. Check the *Callback* checkbox.
    - b. Enter a callback phone number in the Callback Number field.
  11. Click *OK*.
  12. Click *Save and apply changes*.

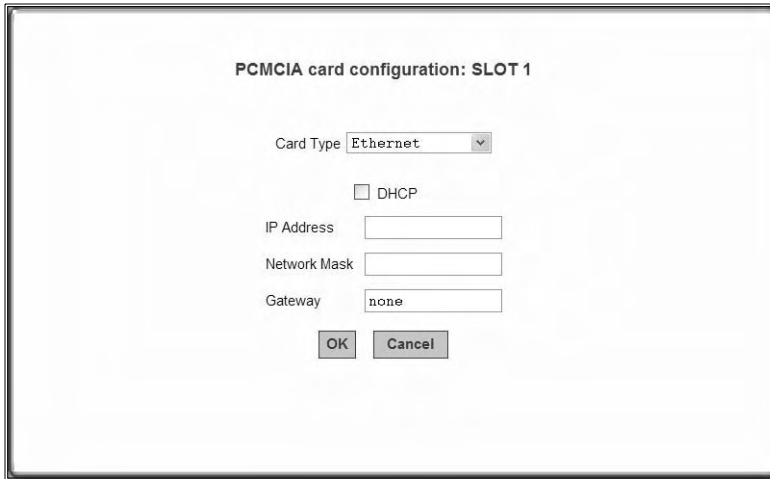
### Configuring an Ethernet LAN PCMCIA card

When an administrative user selects *Ethernet* from the Card Type pull-down menu on the PCMCIA card configuration dialog, the dialog appears as shown in the following figure when the *DHCP* checkbox is checked.



**Figure 6.36: Settings-PCMCIA-Configure-Ethernet or Wireless LAN-DHCP**

The dialog for configuring an Ethernet card displays additional fields when the *DHCP* checkbox is not checked is shown in Figure 6.37.



The screenshot shows a dialog box titled "PCMCIA card configuration: SLOT 1". It contains a "Card Type" dropdown menu with "Ethernet" selected. Below it is a "DHCP" checkbox which is unchecked. There are three text input fields: "IP Address", "Network Mask", and "Gateway". The "Gateway" field contains the text "none". At the bottom of the dialog are "OK" and "Cancel" buttons.

Figure 6.37: Settings-PCMCIA-Configure Ethernet Dialog-Without DHCP

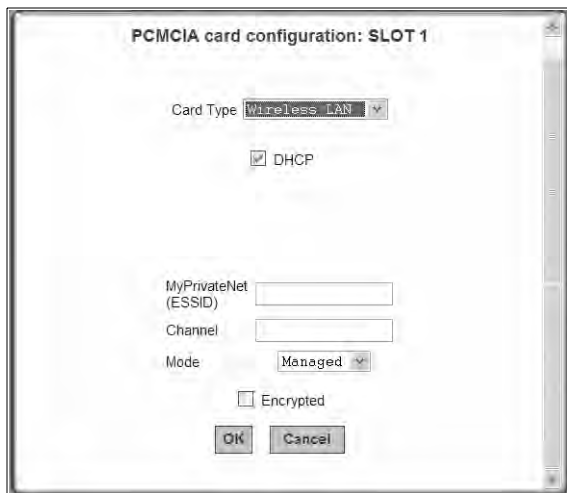
### To configure an Ethernet PCMCIA card:

This procedure assumes that an Ethernet card is inserted into a PCMCIA slot on the OnBoard appliance and the steps under *To begin configuring a PCMCIA card:* on page 124 are complete.

1. Select the *Settings-PCMCIA* menu option.
2. Make sure that *Ethernet* is selected from the Card Type pull-down menu on the PCMCIA card configuration dialog.
3. To enable DHCP, check the *DHCP* checkbox and go to step 5.
4. To define basic network parameters that enable the use of a static IP address, perform 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.
5. Click *OK*.
6. Click *Save and apply changes*.

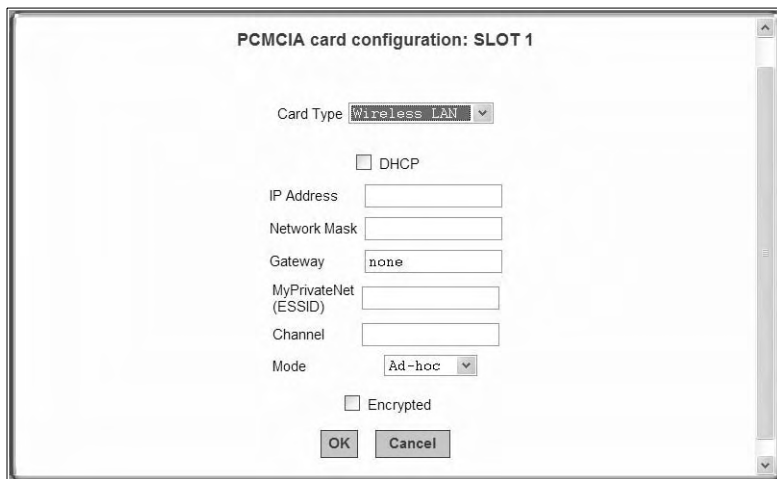
### Configuring a wireless LAN PCMCIA card

When an administrative user selects *Wireless LAN* from the Card Type pull-down menu on the PCMCIA card configuration dialog, the dialog appears as shown in the following figure when the *DHCP* checkbox is checked.



**Figure 6.38: Settings-PCMCIA-Configure-Ethernet or Wireless LAN-DHCP**

As shown in Figure 6.39, the dialog for configuring the Wireless LAN card displays additional fields when the *DHCP* checkbox is not checked.



**Figure 6.39: Settings-PCMCIA-Configure Wireless LAN Dialog Without DHCP**

### **To configure a wireless LAN PCMCIA card:**

This procedure assumes that a wireless LAN card is inserted into a PCMCIA slot on the OnBoard appliance and the steps under *To begin configuring a PCMCIA card:* on page 124 are complete.

1. Select the *Settings-PCMCIA* menu option.

2. Make sure that *Wireless LAN* is selected from the Card Type pull-down menu on the PCMCIA card configuration dialog.
3. To enable DHCP, check the *DHCP* checkbox and go to step 6.
4. 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.
5. Enter a network name in the MyPrivateNet [ESSID] field.
6. Enter a channel in the Channel field.
7. Select either *Managed* or *Ad-hoc* from the Managed pull-down menu.
8. Click *OK*.
9. 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.

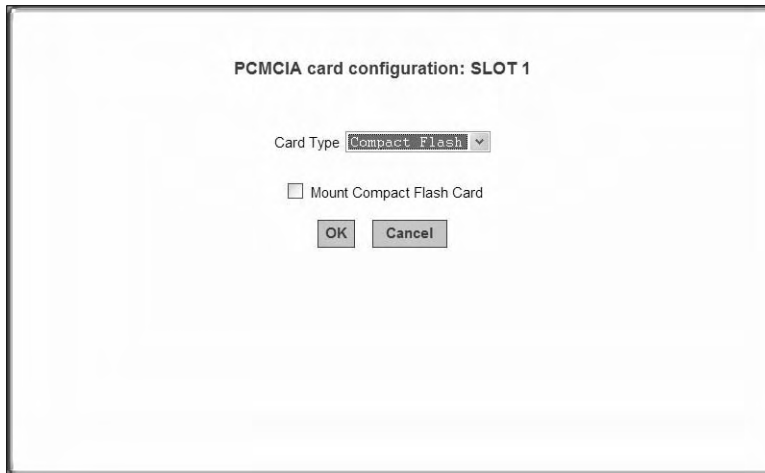


Figure 6.40: Settings-PCMCIA-Configure Flash Dialog: Mount Option Unchecked

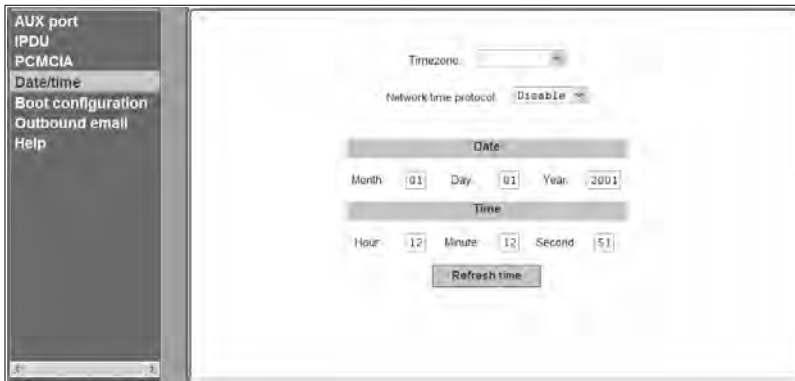
### To configure a compact Flash PCMCIA card:

1. Select the *Settings-PCMCIA* menu option.
2. Make sure that a compact Flash card is inserted into a PCMCIA slot and the steps under *To begin configuring a PCMCIA card*: on page 124 are complete.

3. Select *Compact Flash* from the Card Type pull-down menu on the PCMCIA card configuration dialog.
4. To mount a filesystem from the compact Flash memory, check the *Mount Compact Flash Card* checkbox.
5. Select an option from the File System menu.
6. Click *OK*.
7. Click *Save and apply changes*.

## Configuring system date and time

When an administrative user clicks the *Settings-Date/time* menu option, the following screen appears.



**Figure 6.41: Settings-Date/time Screen**

When *Disable* is selected from the Network Time Protocol menu, Date and Time configuration fields appear, as shown in Figure 6.41, for an administrative user to enter the date and time manually.

An administrative user can use the *Settings-Date/time* screen for configuring the timezone and for specifying how the OnBoard appliance sets its time and date.

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.

### To configure system date and time:

1. Select the *Settings-Date/time* menu option.
2. Select a timezone from the Timezone pull-down menu.
3. To enable the OnBoard appliance 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.



4. 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.
5. Click *OK*.
6. Click *Save and apply changes*.

## Configuring the boot file location

When an administrative user selects the *Settings-Boot configuration* menu option, the following screen appears.



**Figure 6.42: -Boot Configuration Screen**

An administrative user can use the Settings-Boot configuration screen to redefine the location from which the OnBoard appliance boots. By default, the OnBoard appliance boots from an image file that resides on the on-board Flash memory. Booting from the resident software is strongly recommended. Network boots should be reserved only for troubleshooting or upgrading.

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 appliance.

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 appliance handles software upgrades:

- The OnBoard appliance 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 appliance 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 appliance 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.vversion_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 resident removable Flash memory, as described in *To upgrade to a boot image from a network boot in U-boot monitor mode*: on page 277.

### **To boot from a boot server, 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 appliance.
- An upgraded OnBoard appliance boot image file must be downloaded and must be available on the boot server.

- The OnBoard appliance must have a fixed IP address.

**Table 6.8: Boot Configuration Fields and Options**

| Field or Value Name          | Description                                                                                                                                                                                                                                                                                                                                        |
|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| OnBoard appliance IP address | A new IP address for the OnBoard appliance.                                                                                                                                                                                                                                                                                                        |
| Watchdog timer               | Whether the watchdog timer is active. Choices are: <ul style="list-style-type: none"> <li>• InActive</li> <li>• Active</li> </ul> If the watchdog timer is active, the OnBoard appliance reboots if the software crashes. See <i>To configure OnBoard appliance boot</i> : on page 135 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.                                                                                                                                                                                                                                                                                                  |

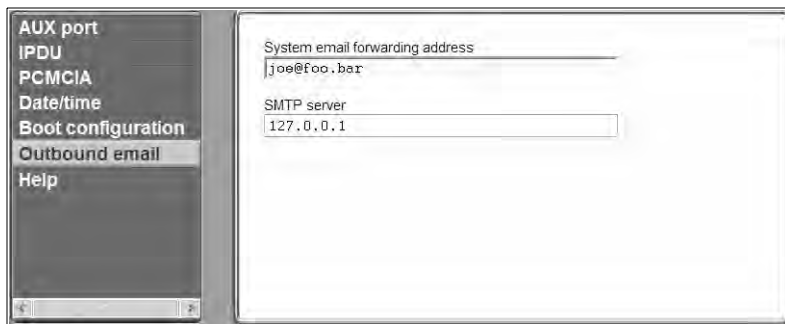
### To configure OnBoard appliance boot:

1. Select the *Settings-Boot configuration* menu option. The Boot Configuration form appears.
2. Enter the IP address of the OnBoard appliance in the OnBoard appliance IP Address field.
3. Accept or change the option in the Watchdog Timer field (Inactive or Active).
4. Select 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 outbound email

When an administrative user selects the *Settings-Outbound* menu option, the administrative user can configure an SMTP server and an email address for an administrator to receive email from the system, such as those generated by the cron daemon.

Figure 6.43 shows the screen that appears when an administrative user clicks the Outbound email option under Settings.



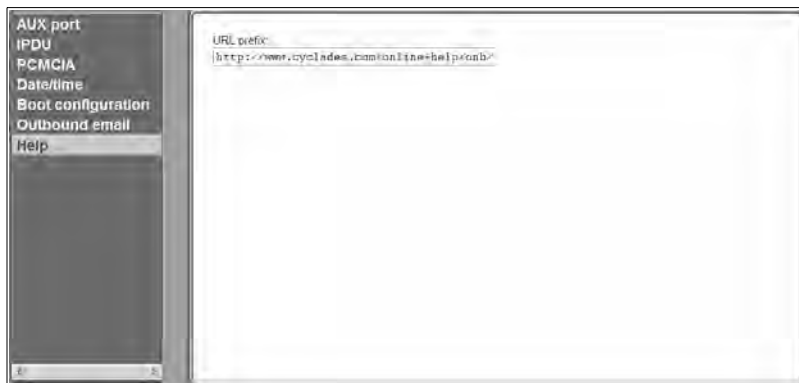
**Figure 6.43: Settings-Outbound Email Screen**

#### To configure a recipient for OnBoard appliance system email:

1. Log into the *Web Manager* as an administrative user.
2. Select the *Settings-Outbound email* menu option. The Outbound email configuration screen appears.
3. Enter the email address in the System email forwarding address field.
4. Enter the DNS name or the IP address for the SMTP server.
5. Click *Save and apply changes*.

### Configuring an alternate help file location

When an administrative user selects the *Settings-Help* menu option, the following screen appears.



**Figure 6.44: Settings-Help Screen**

The Help button on the Web Manager looks for help files in the location specified here. The OnBoard appliance help is located at URL specified on the screen by default.

If an OnBoard appliance administrator downloads the help files from the specified ftp server onto another web server or other directory that is available to users, then the administrative user can change the URL in the URL Prefix field to point the Help button to the new location for the files.

### To specify a new location for OnBoard appliance help files:

1. Download the compressed help file from `ftp://ftp.cyclades.com/pub/cyclades/alterpath/onb/doc/OnBoard_online_hlp.zip`.
2. Extract the files and put them into the desired directory under the web server's root directory on a publicly accessible web server. For example the following command line would work on a workstation running a UNIX-based operating system.

```
cd $WEB_SERVER_ROOT/
gunzip OnBoard_online_hlp.zip
```

By default, the online help files are expanded into a directory named `onboard` that is created under the directory where the zip file is located. If desired, move the `onboard` directory name to another location.

3. Log into the Web Manager as an administrative user, then select the *Settings-Help* menu option. The Help configuration screen appears.
4. In the URL prefix field, enter the URL of the help files on the server where you installed them. The following example would work for a web server named `remoteadmin`.

```
http://www.remoteadmin.com/onboard
```

The software adds the name of the `onboard` directory to the URL prefix and opens the `index.html` file that launches the help.

5. Click *Save and apply changes*.

## Web Manager Config Menu Options

Table 6.9 lists the options that appear when an administrative user selects the *Config* top menu option and provides links to where the options are described.

**Table 6.9: Options Under Config**

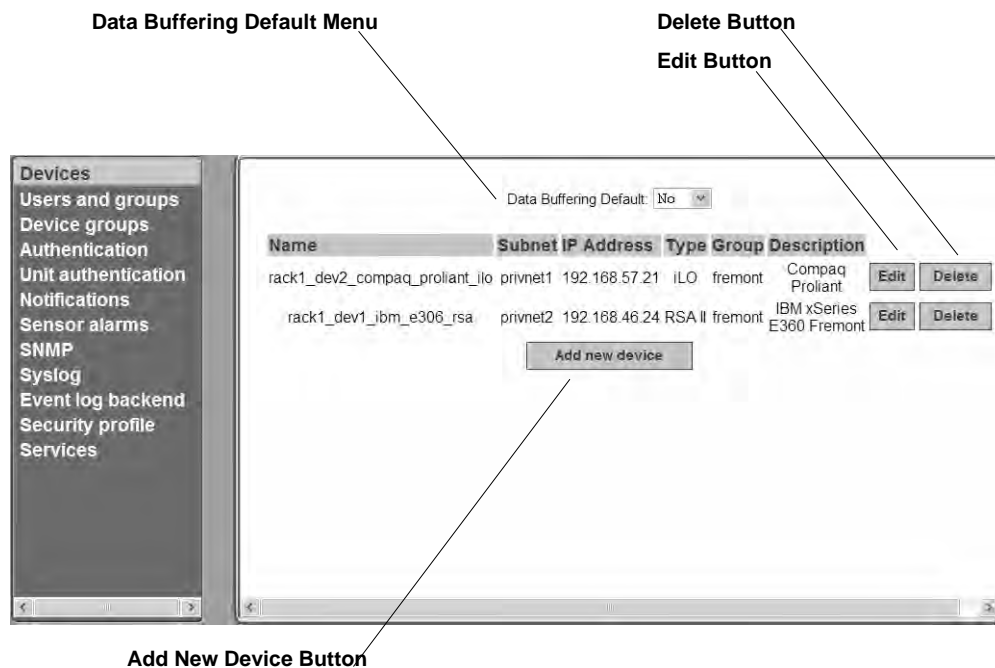
| Option              | Where Described                                                                   |
|---------------------|-----------------------------------------------------------------------------------|
| Devices             | <i>Configuring devices</i> on page 138                                            |
| Users and groups    | <i>Configuring Users and Groups</i> on page 140                                   |
| Device groups       | <i>Configuring device groups</i> on page 143                                      |
| Authentication      | <i>Configuring authentication servers</i> on page 144                             |
| Unit authentication | <i>Configuring an authentication method for the OnBoard appliance</i> on page 151 |
| Notifications       | <i>Configuring Notifications</i> on page 152                                      |
| Sensor alarms       | <i>Configuring Sensor Alarms</i> on page 155                                      |

**Table 6.9: Options Under Config (Continued)**

| Option            | Where Described                                                     |
|-------------------|---------------------------------------------------------------------|
| SNMP              | <i>Configuring SNMP</i> on page 161                                 |
| Syslog            | <i>Configuring Logging of System Messages (Syslogs)</i> on page 166 |
| Event log backend | <i>Configuring the Event Log Backend</i> on page 168                |
| Security profile  | <i>Selecting or Configuring a Security Profile</i> on page 169      |
| Services          | <i>To configure services:</i> on page 169                           |

## Configuring devices

When an administrative user selects the *Config-Devices* menu option, the following screen appears.

**Figure 6.45: Config-Devices Screen**

An administrative user can use the Config-Devices screen for configuring devices connected to the OnBoard appliance and for configuring data buffering.

The selection on the Data Buffering Default menu sets a default for data buffering for all devices, either Yes or No. When configuring individual devices, the administrative user can select either Default, Yes or No to configure data buffering for the specific device.

Clicking the Add new device or Edit buttons bring up a screen for configuring devices.

---

**CAUTION:**All devices connected to the private Ethernet ports of the OnBoard appliance must have a previously-configured private subnet name assigned. If not, the device can only be accessed if it is connected to the public network, a highly unlikely scenario and not recommended.

---

The Web Manager displays devices in the order in which they are configured. An OnBoard administrator can configure device lists to appear in alphabetical order using the `cycli` utility. See *Changing the Sort Order of Device Listings* on page 83.

## Adding a device

Make sure the following are complete.

- A private subnet has been created.
- An administrator has followed the procedure under *To use the `onbdtemplate` utility to create a new template*: on page 234 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 SP or device.

### To add a device:

1. Log into the Web Manager as an administrative user.
2. Select the *Config-Devices* menu option.
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. If device groups have been configured, select the device group from the Device group pull-down menu.
7. Select the device type from the Type pull-down menu.
8. Select a data buffering option, *Yes*, *No* or *Default* from the Data buffering pull-down menu.
9. Select a private subnet name from the Private subnet name/Addr field.
10. Enter the real IP address for the device in the Device IP address field.
11. If a virtual address has been configured, enter a virtual IP address for the device in the Virtual IP address field.
12. Enter a device description in the Description field.
13. Select an authentication type from the Authentication type pull-down menu.
14. Select a command template or *no template* from the Command template pull-down menu.
15. Click *OK*.
16. Click *Save and apply changes*.

## Configuring Users and Groups

When an administrative user selects the *Config-Users and groups* menu option, a screen like the one shown in the following figure appears.

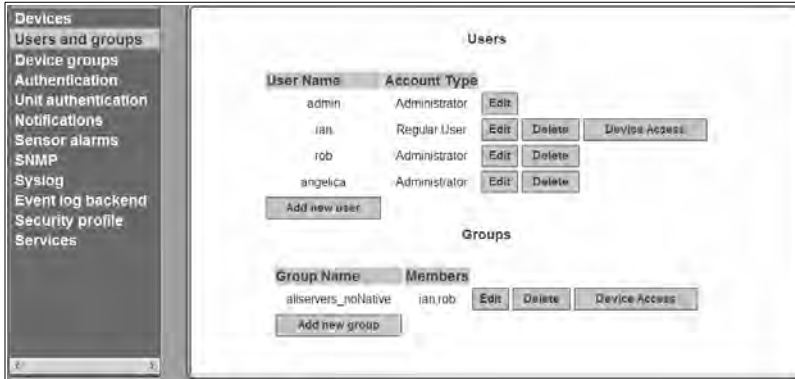


Figure 6.46: Config-Users and Groups Screen

An administrative user can use the Config-Users and groups screen for adding users and groups and for authorizing users and groups to access devices through the OnBoard appliance. The administrative user may also choose to add additional users who can administer the OnBoard appliance as administrative users by adding them to the admin group.

### Configuring users

See Table 4.5 on page 29 for descriptions of the parameters that can be set on the dialogs that appear when the *Add a regular user* or *Edit* options are selected. Clicking the *Delete* button deletes the user without bringing up a confirmation dialog.

Clicking the *Device Access* button brings up the Edit <username's> device access privileges screen.

If no configured devices remain to be assigned to the user, the *Add new device button* does not appear.

### Configuring groups

Clicking the *Add new group button* or clicking the *Edit* button for an existing group brings up a screen for configuring groups. Clicking the *Delete* button deletes the group without bringing up a confirmation dialog.

Clicking the *Device Access* button brings up the Edit groupname's device access privileges screen.

If no configured devices remain to be assigned to the group, the *Add new device button* does not appear. Clicking the *Add new device button* brings up a screen with the fields and menu options for configuring the group's access to a device.



**To create and authorize a user for device management:**

1. Log into the Web Manager as an administrative user.
2. Select the *Config-Users and groups* menu option.
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: 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 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.
2. Select the *Config-Users and groups* menu option.
3. 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*.
4. 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 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*.

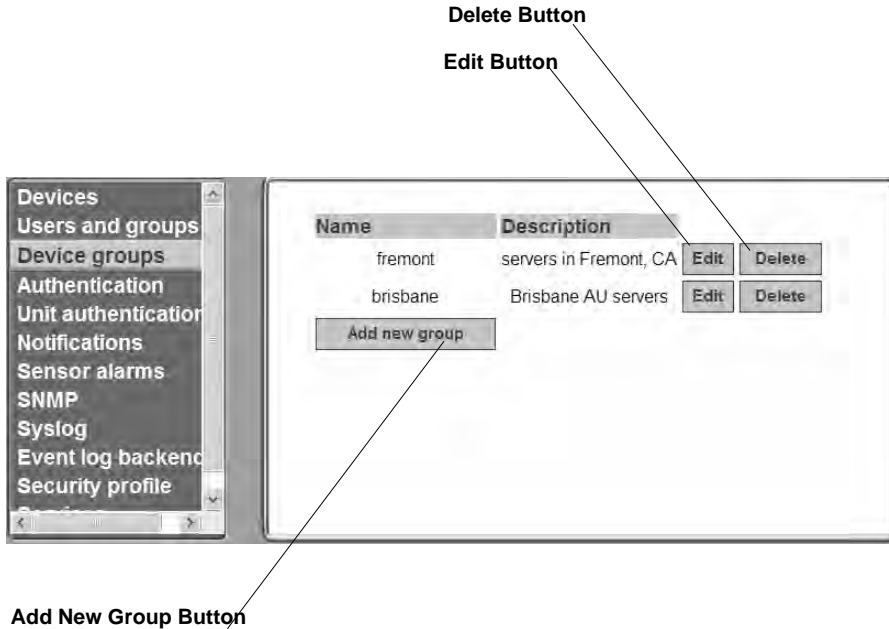
**To create and authorize user groups for device management:**

1. Log into the Web Manager as an administrative user.
2. Select the *Config-Users and groups* menu option.
3. 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 usernames with commas and no spaces.
  - e. Click *OK*. The Edit <groupname's> device access privileges screen appears.
4. 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 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.
5. Click *OK*.
6. Click *Save and apply changes*.

## Configuring device groups

When an administrative user selects the *Config-Device groups* menu option, the following screen appears.



**Figure 6.47: Config-Device Groups Screen**

The administrative user can use the Config-Device groups screen for configuring optional device groups. If device groups are added, an administrator can add a device to a group during configuration of the device. See *Configuring devices* on page 138.

### To configure device groups:

1. Log into the Web Manager as an administrative user.
2. Select the *Config-Device groups* menu option.
3. Select *Add new group* or *Edit*.
4. Add or modify a device group by entering or modifying the group name and the description.
5. Click *OK*.
6. Click *Save and apply changes*.

## Configuring Authentication

The administrative user must decide whether to require authentication for logins into the OnBoard appliance or 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 6.10: Tasks for Authentication Configuration**

| Task                                                          | Where Documented                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Configure authentication servers                              | <p><i>Configuring authentication servers</i> on page 144</p> <ul style="list-style-type: none"> <li>• <i>Configuring a Kerberos authentication server</i> on page 145</li> <li>• <i>Configuring an LDAP authentication server</i> on page 146</li> <li>• <i>Configuring a NIS authentication server</i> on page 147</li> <li>• <i>Configuring a RADIUS authentication server</i> on page 148</li> <li>• <i>Configuring an SMB authentication server</i> on page 149</li> <li>• <i>Configuring a TACACS+ authentication server</i> on page 150</li> </ul> |
| Specify an authentication method for OnBoard appliance logins | <p><i>Configuring an authentication method for the OnBoard appliance</i> on page 151</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Specify authentication for devices                            | <ul style="list-style-type: none"> <li>• <i>Configuring devices</i> on page 138</li> <li>• <i>Selecting or Configuring a Security Profile</i> on page 169</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                     |

### Configuring authentication servers

When an administrative user selects the *Config-Authentication* menu option, a screen appears for configuring authentication servers.

The default authentication type is Local, and if it is selected, it requires no configuration. 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.

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 138 for how devices are assigned an authentication method.
- The OnBoard appliance, if it is subsequently configured to use that authentication method. See *Configuring an authentication method for the OnBoard appliance* on page 151 for how the OnBoard appliance is assigned an authentication method.

## Configuring a Kerberos authentication server

When an administrative user selects the *Config-Authentication* menu option and selects *Kerberos* from the Authentication Type pull-down menu, additional fields appear on the Config-Authentication screen for configuring the Kerberos server.

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 Kerberos Realm Domain Name and the Kerberos Server IP address, which display when the Kerberos authentication type is selected.

---

**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 appliance to be synchronized with the time on the KDC.

---

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 appliance 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 appliance, accounts for all users who need to log into the OnBoard appliance to administer connected devices
- If Kerberos authentication is specified for devices, accounts for users who need access to connected devices

Configure an authentication server when the OnBoard appliance or any of its connected devices is configured to use the Kerberos authentication method or any of its variations (Kerberos, Local/Kerberos, Kerberos/Local or Kerberos Down/Local).

### To configure a Kerberos authentication server:

1. Log into the Web Manager as an administrative user.
2. Make sure entries for the OnBoard appliance and the Kerberos server exist in the OnBoard appliance's `/etc/hosts` file.
  - a. Select the *Network-Host Table* menu option. The Host Table form appears.
  - b. Add an entry for OnBoard appliance (if needed) and add an entry for the Kerberos server.
3. Make sure that timezone and time and date settings are synchronized between the OnBoard appliance 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 appliance and the Kerberos server to use the same NTP server.

---

- a. Follow the procedure under *Configuring system date and time* on page 132 to set the timezone, date and time.
- b. Work with the authentication server's administrator to synchronize the time and date between the OnBoard appliance and the server.
4. Select the *Config-Authentication* menu option.
5. Select *Kerberos* from the Authentication Type pull-down menu. The Kerberos configuration fields display.
6. Enter the IP address of the Kerberos server in the Kerberos Server IP address field.
7. Enter the domain name of the Kerberos realm in the Kerberos Realm Domain Name field.
8. Click *Save and apply changes*.

## Configuring an LDAP authentication server

When an administrative user selects the *Config-Authentication* menu option and selects *LDAP* from the Authentication Type pull-down menu, additional fields appear on the Config-Authentication screen for configuring the LDAP server.

The following two fields and menu display when the LDAP authentication type is selected:

- LDAP Server IP address
- LDAP Base-The distinguished name of the search base

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.

The domain name is specified as shown in the following example. For the LDAP domain name cyclades.com, the correct entry would be: dc=cyclades,dc=com.

- Secure LDAP pull-down menu. Options are Off, On and Start TLS.

You can enter information in the following three fields, but entries are not required:

- LDAP User Name
- LDAP Password
- LDAP Login Attribute (defaults to UID)

Configure an authentication server when the OnBoard appliance or any of its connected devices is configured 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 appliance 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 appliance, accounts for all users who need to log into the OnBoard appliance.
- If LDAP authentication is specified for devices, accounts for users who need access to the connected devices.

See *Configuring group authorization for LDAP authentication* on page 84 for how to manually configure group authorizations with LDAP authentication, if desired.

### **To configure an LDAP authentication server:**

1. Log into the Web Manager as an administrative user.
2. Select the *Config-Authentication* menu option.
3. 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.
4. Enter the IP address of the LDAP server in the LDAP Server field.
5. 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.
6. Replace the default domain name with the name of your LDAP domain.
7. Pick an option from the Secure LDAP pull-down menu.
8. Enter an optional username in the LDAP User Name field.
9. Enter an optional password in the LDAP Password field.
10. Enter an optional login attribute in the LDAP Login Attribute field.
11. Click *Save and apply changes*. The changes are stored in `/etc/ldap.conf` on the OnBoard appliance.

## **Configuring a NIS authentication server**

When an administrative user selects the *Config-Authentication* menu option and selects *NIS* from the Authentication Type pull-down menu, additional fields appear on the Config-Authentication screen for configuring the NIS server.

Configure a NIS authentication server when the OnBoard appliance or any of its connected devices is configured to use the NIS authentication method or any of its variations (NIS/DownLocal, Local/NIS or NIS/Local).

The administrative user must obtain the needed information about the NIS server from the server's administrator and configure the server by filling in the NIS Domain Name and NIS Server IP fields that display when the NIS authentication type is selected on the Config-Authentication screen.

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 appliance and connected devices know the passwords assigned to the accounts:

- An account for admin

- If NIS authentication is specified for the OnBoard appliance, accounts for all users who need to log into the OnBoard appliance
- If NIS authentication is specified for devices, accounts for users who need access to the connected devices

**To configure a NIS authentication server:**

1. Log into the Web Manager as an administrative user.
2. Select the *Config-Authentication* menu option.
3. Select *NIS* from the Authentication Type pull-down menu. The NIS fields display.
4. Enter the NIS domain name in the NIS Domain Name field.
5. Enter the IP address of the NIS server in the NIS Server IP field.
6. Click *Save and apply changes*.

**Configuring a RADIUS authentication server**

When an administrative user selects the *Config-Authentication* menu option and selects *Radius* from the Authentication Type pull-down menu, additional fields appear on the Config-Authentication screen for configuring the Radius server.

The administrative user must obtain the needed information about the RADIUS server from the server's administrator and configure the server by filling in the 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

Configure a RADIUS authentication server when the OnBoard appliance or any of the connected devices is configured 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 appliance 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 appliance, accounts for all users who need to log into the OnBoard appliance.



- If RADIUS authentication is specified for devices, accounts for users who need access to the connected devices.

See *Configuring group authorization for RADIUS authentication* on page 86 for how to manually configure group authorizations with RADIUS authentication.

#### **To configure a RADIUS authentication server:**

1. Log into the Web Manager as an administrative user.
2. Select the *Config-Authentication* menu option.
3. Select *Radius* from the Authentication Type pull-down menu.
4. Enter the IP address of the first or only authentication server in the First Authentication Server field.
5. Enter the IP address of a second authentication server (if available) in the Second Authentication Server field.
6. Enter the secret in the Secret field.
7. Enter one or more time-out values in the Timeout field.
8. Enter a number of retries in the Retries field.
9. Click *Save and apply changes*.

### **Configuring an SMB authentication server**

When an administrative user selects the *Config-Authentication* menu option and selects *SMB* from the Authentication Type pull-down menu, additional fields appear on the Config-Authentication screen for configuring the SMB server.

Configure an SMB authentication server when the OnBoard appliance 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).

The administrative user must obtain the needed information about the SMB server from the server's administrator and configure the server by filling in the Domain, Primary Domain Controller and Secondary Domain Controller fields that display when the SMB authentication type is selected.

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 appliance 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 appliance, accounts for all users who need to log into the OnBoard appliance
- If SMB authentication is specified for devices, accounts for users who need access to the connected devices

**To configure an SMB authentication server:**

1. Log into the Web Manager as an administrative user.
2. Select the *Config-Authentication* menu option.
3. Select *SMB* from the Authentication Type pull-down menu.
4. Enter the SMB domain name in the Domain field.
5. Enter the IP address of the primary domain controller in the Primary Domain Controller field.
6. Enter the IP address of the secondary domain controller in the Secondary Domain Controller field.
7. Click *Save and apply changes*.

**Configuring a TACACS+ authentication server**

When an administrative user selects the *Config-Authentication* menu option and selects *TACACS+* from the Authentication Type pull-down menu, additional fields appear on the *Config-Authentication* screen for configuring the TACACS+ server.

Configure a TACACS+ authentication server when the OnBoard appliance 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*).

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 the following 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

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 appliance and connected devices know the passwords assigned to the accounts:

**Prerequisites for a TACACS+ server configuration**

To configure a TACACS+ authentication server, you must prepare for the following:

- An account for admin or other administrative user.

- If TACACS+ authentication is specified for the OnBoard appliance, accounts for all users who need to log into the OnBoard appliance.
- If TACACS+ authentication is specified for devices, accounts for users who need access to the connected devices.

**To configure a TACACS+ authentication server:**

1. Log into the Web Manager as an administrative user.
2. Select the *Config-Authentication* menu option.
3. Select TACACS+ from the Authentication Type pull-down menu.
4. Enter the IP address of the first authentication server in the First Authentication Server field.
5. Enter the IP address of a second authentication server in the Second Authentication Server field.
6. Enter the IP address of the first accounting server in the First Accounting Server field.
7. Enter the IP address of the second accounting server in the Second Accounting Server field.
8. Enter the secret in the Secret field.
9. Check or leave unchecked the *Enable Raccess Authorization* checkbox.
10. Enter one or more time-out values in the Timeout field.
11. Enter a number of retries in the Retries field.
12. Click *Save and apply changes*.

## Configuring an authentication method for the OnBoard appliance

When an administrative user selects the *Config-Unit Authentication* menu option, 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 appliance.



**Figure 6.48: Default Config-Unit Authentication Screen**

By default Local authentication is in effect, and no configuration is required.

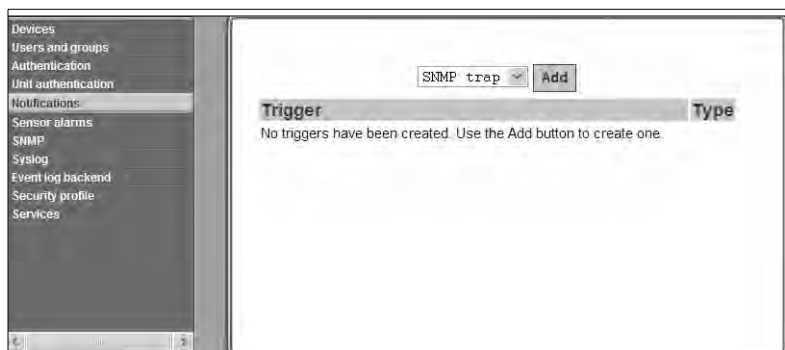
This screen configures an authentication method for logins into the OnBoard appliance. An authentication server must be available and must be configured as described under *Configuring authentication servers* on page 144.

**To configure an authentication method for OnBoard appliance logins:**

1. Log into the Web Manager as an administrative user.
2. Select the *Config-Unit authentication* menu option.
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 selects the *Config-Notifications* menu option, a screen like the one shown in Figure 6.49 appears. The administrative user can use this screen for defining alarm triggers to generate notifications when the specified events occur. The syslogd filters what kinds of messages and takes the specified action based on the content of the messages. The administrative user specifies the notices to be sent by SNMP trap, pager or email.



**Figure 6.49: Default Config-Notifications Screen**

The screen shown in Figure 6.49 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 dialog that appears next has different fields and menu options depending on which notification method was selected.

The following table shows the fields for configuring any type of notification.

**Table 6.11: Values for Configuring Any Type of Notification**

| Checkbox, Field or Menu Name            | Description |
|-----------------------------------------|-------------|
| Scan device console session for matches | As stated   |

**Table 6.11: Values for Configuring Any Type of Notification (Continued)**

| Checkbox, Field or Menu Name | Description                                                                                                                                                                                                                                                         |
|------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name                         | The name for the trigger                                                                                                                                                                                                                                            |
| Alarm trigger                | A function and a regular expression in syslog-ng format. Use the format: <code>function('regular_expression')</code> . For example, the following example searches system messages for Denied, denied, Fail and fail:<br><code>match('[Dd]enied   [Ff]ail');</code> |

## Configuring SNMP trap notifications

If the Simple Network Management Protocol (SNMP) service is enabled on the OnBoard appliance, the OnBoard appliance administrator can use the SNMP Trap Add dialog to send notifications about significant events to an SNMP management application, such as HP Openview, Novell NMS, IBM NetView or Sun Net Manager.

The SNMP Trap Add dialog may be used for configuring an alarm trigger and a SNMP trap notification to be sent if the specified alarm trigger occurs.

### To configure SNMP trap notifications:

1. Log into the Web Manager as an administrative user.
2. Select the *Config-Notifications* menu option.
3. Select *SNMP trap* from the pull-down menu.
4. Select *Add*.
5. Check or leave unchecked the checkbox next to *Scan device console session for matches*.
6. Enter a name for the trigger in the Name field.
7. Use syslog-ng syntax to specify an event to trigger the alarm in the Alarm trigger field.
8. Select a protocol from the Protocol menu.
9. Enter an OID in the OID field.
10. Select one of the trap designators from the Generic trap type pull-down menu. If the enterpriseSpecific trap designator is selected, you are prompted for a specific trap number.
11. If either SNMP v1 or v2c is selected, enter a community name in the Community field.
12. If SNMP v3 is selected, perform the following steps.
  - a. Enter a username in the User field.
  - b. Select an authentication level from the Auth Level pull-down menu.
  - c. If Auth or Auth & crypt are selected, select an option from the Auth Level menu.
  - d. Enter an optional password in the Auth password field.
  - e. If Auth & crypt is selected, select an option from the Encryption menu.
  - f. Enter an optional password in the Crypt password field.

13. Enter an SNMP server IP address or DNS name in the SNMP server field.
14. Enter any desired text in the Body field.
15. Click *OK*.
16. Click *Save and apply changes*.

## Configuring pager notifications

The OnBoard appliance administrator can use the Pager Add dialog to can be used to configure an alarm trigger and a pager notification to be sent if the specified alarm trigger occurs. For pager notifications, the administrative user needs to configure the values in Table 6.12, in addition to the values in Table 6.11 on page 152.

**Table 6.12: Fields for Configuring a Pager Notification**

| Field or Menu Name | Notes                                                 |
|--------------------|-------------------------------------------------------|
| 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) username             |
| SMS server         | The SMS server's IP address or DNS name               |
| SMS port           | The SMS port number                                   |

### To configure pager notifications:

1. Log into the Web Manager as an administrative user.
2. Select the *Config-Notifications* menu option.
3. Select *Pager* from the pull-down menu.
4. Select *Add*.
5. Check or leave unchecked the checkbox next to *Scan device console session for matches*.
6. Enter a name for the notification in the Name field.
7. Use syslog-ng syntax to specify an event to trigger the alarm in the Alarm trigger field.
8. Enter a pager or phone number in the Pager/phone number field.
9. Enter the desired text in the Text field.
10. Enter a username in the SMS username field.
11. Enter the IP address for an SMS server in the SMS server field.
12. Enter an SMS port in the SMS port field.
13. Click *OK*.
14. Click *Save and apply changes*.

## Configuring email notifications

The OnBoard appliance administrator can use the Email Add Dialog to configure an alarm trigger and an email notification to be sent if the specified alarm trigger occurs. For email notifications, the administrative user needs to configure the values in Table 6.13, in addition to the values in Table 6.11 on page 152.

**Table 6.13: Fields for Configuring an Email Notification**

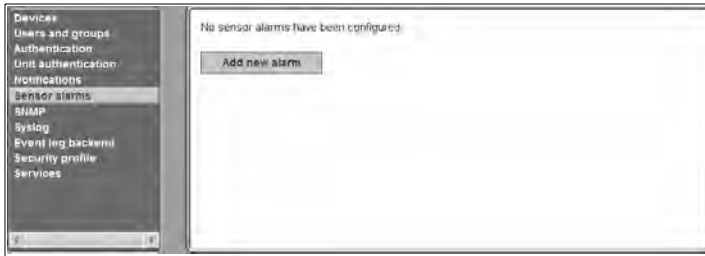
| Field or Menu Name | Notes                                                             |
|--------------------|-------------------------------------------------------------------|
| To                 | The email address of the user account to receive the notification |
| From               | The sender's email address                                        |
| Subject            | Summary text to describe the event triggering the email           |
| Body               | Description of the event                                          |

### To configure an email notification:

1. Log into the Web Manager as an administrative user.
2. Select the *Config-Notifications* menu option.
3. Select *Email* from the pull-down menu.
4. Select *Add*.
5. Check or leave unchecked the checkbox next to *Scan device console session for matches*.
6. Enter a name for the notification in the Name field.
7. Use syslog-ng syntax to specify an event to trigger the alarm in the Alarm trigger field.
8. Enter a destination email address in the To field.
9. Enter a source email address in the From field.
10. Enter a subject that describes the alarm trigger in the Subject field.
11. Enter the desired text for the email message in the Body field.
12. Click *OK*.
13. Click *Save and apply changes*.

## Configuring Sensor Alarms

When an administrative user selects the *Config-Sensor alarms* menu option, the screen shown in Figure 6.50 appears. The administrative user can use this screen to configure the OnBoard appliance 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 6.50: Default Config-Sensor Alarms Screen**

Figure 6.51 shows the screen that appears when the *Add new alarm* button is clicked. As shown, by default, the Syslog message option is selected from the Action menu.

**Figure 6.51: Default Config-Sensor Alarms Screen**

### To begin configuring a sensor alarm:

1. Log into the Web Manager as an administrative user.
2. Select the *Config-Sensor Alarms* menu option.
3. Click the *Add new alarm* button. The add sensor alarm dialog appears.
4. Select a device from the Device pull-down menu.
5. Specify the sensor to monitor in the Sensor field.
6. Select a condition to trigger the sensor alarm from the Condition pull-down menu.
7. When the condition selected in step 6 is inside or outside a range, specify the range in the Range fields.
8. Specify a polling interval and choose minutes or hours from the Interval pull-down menu.
9. Select the desired notification action from the Action pull-down menu.
10. Enter a comment, if desired, in the Comment field.



## 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 6.51.

The screenshot shows a web form for configuring a Syslog message sensor alarm action. At the top, the 'Action' dropdown menu is set to 'Syslog message'. Below it is a 'Comment' text input field. The section is titled 'Syslog message'. Underneath, the 'Priority' dropdown menu is set to '4 - WARNING'. Below that is a 'Body' text input field. At the bottom right of the form are 'OK' and 'Cancel' buttons.

**Figure 6.52: Config-Sensor Alarms Syslog Message Fields**

### To configure a Syslog message sensor alarm action:

1. Log into the Web Manager as an administrative user.
2. Select the *Config-Sensor Alarms* menu option.
3. Select *Syslog message* from the Action menu.
4. Select a priority from the Priority menu.
5. Enter text as desired in the Body field.
6. Click *OK*.
7. Click *Save and apply changes*.

## Configuring the SNMP trap sensor alarm action

Figure 6.53 shows the fields that appear when SNMP trap is selected on the Action menu on the Config-Sensor Alarms screen.

The screenshot shows a web form for configuring an SNMP trap sensor alarm action. At the top, the 'Action' dropdown menu is set to 'SNMP trap'. Below it is a 'Comment' text input field. The section is titled 'SNMP trap'. Underneath, the 'Protocol' dropdown menu is set to 'SNMP v1'. Below that is an 'OID' text input field. The 'Generic trap type' dropdown menu is set to 'coldStart'. Below that is a 'Community' text input field. Below that is a 'Server' text input field. At the bottom is a 'Body' text input field. At the bottom right of the form are 'OK' and 'Cancel' buttons.

**Figure 6.53: Config-Sensor Alarms SNMP Trap Fields for V1 and V2c**

The fields that appear when SNMP v1 and v2 are selected are the same, but when SNMP v3 is selected other fields appear, as shown in Figure 6.54.

The image shows a dialog box titled "SNMP trap" with several configuration fields. The "Protocol" field is a dropdown menu set to "SNMP v3". The "OID" field is an empty text box. The "Generic trap type" field is a dropdown menu set to "coldStart". The "User" field is an empty text box. The "Auth Level" field is a dropdown menu set to "No auth". The "Server" field is an empty text box. The "Body" field is a larger empty text box. At the bottom right of the dialog are "OK" and "Cancel" buttons.

**Figure 6.54: Config-Sensor Alarms SNMP Trap Fields for V3**

See *SNMP on the OnBoard Appliance* on page 35 for values to define SNMP traps.

**To configure an SNMP trap sensor alarm action:**

1. Log into the Web Manager as an administrative user.
2. Select the *Config-Sensor Alarms* menu option.
3. Select *SNMP trap* from the Action menu.
4. Select a protocol from the Protocol menu.
5. Enter the OID in the OID field.
6. Select a trap type from the Generic trap type field.
7. If either v1 or v2 is selected in step 6, enter the name of a community in the Community field.
8. If v3 is selected in step 6, perform the following steps.
  - a. Enter the username required for authentication in the User field.
  - b. Select an authentication level from the Auth Level pull-down menu.
  - c. If Auth or Auth & Crypt are selected, select an authentication method from the Auth Method pull-down menu.
  - d. If Auth or Auth & Crypt are selected, enter the authentication password in the Auth password field.
  - e. If Auth & Crypt is selected, select an encryption method from the Encryption pull-down menu.
  - f. If Auth & Crypt is selected, enter the appropriate password for the encryption method in the Crypt pass field.
  - g. Enter the IP address or DNS-resolvable name of the SNMP manager in the Server field.
  - h. Enter any desired text in the Body field.
9. Click *OK*.
10. Click *Save and apply changes*.

## Configuring a pager sensor alarm action

Figure 6.55 shows the fields that appear when Pager is selected on the Action menu on the Config-Sensor Alarms screen that is shown in Figure 6.51.

The screenshot shows a web form for configuring a pager sensor alarm action. At the top, there is a dropdown menu labeled 'Action' with 'Pager' selected. Below it is a text input field for 'Comment'. A section header 'Pager' is followed by several input fields: 'Pager/phone number', 'SMS username', 'SMS server', 'SMS port', and 'Message'. At the bottom of the form are two buttons: 'OK' and 'Cancel'.

**Figure 6.55: Config-Sensor Alarms Pager Message Fields**

**Table 6.14: Fields for Configuring Pager Sensor Alarms**

| Field or Menu Name | Notes                                               |
|--------------------|-----------------------------------------------------|
| Pager/phone number | Pager or phone number.                              |
| SMS username       | SMS username.                                       |
| 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. Log into the Web Manager as an administrative user.
2. Select the *Config-Sensor Alarms* menu option.
3. Select *Pager* from the Action menu.
4. Enter the phone number of the pager or phone to be contacted in the Pager/phone number field.
5. Enter the username required for authentication in the SMS username field.
6. Enter the IP address of the SMS server in the SMS server field.
7. Enter the SMS port number in the SMS port field.
8. Enter any desired message in the Message field.
9. Click *OK*.
10. Click *Save and apply changes*.

## Configuring an email sensor alarm action

Figure 6.56 shows the fields that appear when Email is selected on the Action menu on the Config-Sensor Alarms screen that is shown in Figure 6.51.

The screenshot shows a dialog box for configuring an email sensor alarm action. At the top, there is a dropdown menu for 'Action' with 'Email' selected, and a text input field for 'Comment'. Below this is a section header 'Email'. Underneath are three text input fields for 'From:', 'To:', and 'Subject:'. A large text area for 'Body:' follows. At the bottom right, there are 'OK' and 'Cancel' buttons.

**Figure 6.56: Config-Sensor Alarms Email Message Fields**

**Table 6.15: 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. Log into the Web Manager as an administrative user.
2. Select the *Config-Sensor Alarms* menu option.
3. Select *Email* from the Action menu.
4. Enter the sender's email address in the From field.
5. Enter the recipient's email address in the To field.
6. Enter a string that identifies the alarm in the Subject field.
7. Enter an explanatory message for the alarm in the Body field.
8. Click *OK*.
9. Click *Save and apply changes*.

## Configuring SNMP

Figure 6.57 shows the screen that appears when an administrative user selects the *Config-SNMP* menu option. The administrator can use this screen to configure SNMP access for the OnBoard appliance and for connected devices.



Figure 6.57: Config-SNMP Configuration Screen

**NOTE:** For SNMP to work you need to ensure that the selected security profile enables the SNMP service (by checking the 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.

### Configuring SNMP information settings

Under the OnBoard appliance information settings heading on the Config-SNMP screen shown in Figure 6.57, clicking the *Edit* button enables the administrative user to change the configured values. The Edit button brings up the screen shown below.



Figure 6.58: Config-SNMP: Edit OnBoard appliance Information Settings

### To configure OnBoard appliance SNMP information:

1. Log into the Web Manager as an administrative user.
2. Select the *Config-SNMP* menu option.
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

The names of all configured devices and the OnBoard appliance itself are listed under the Servers SNMP configuration heading on the Config-SNMP screen.

Pressing the SNMP Configure button next to the name of a device brings up a screen like the one shown in the following figure.

**Device sp1 SNMP settings**

---

**Service Processor SNMP setting**

Device alias: sp1                      IP address: 172.20.0.2  
 SNMP protocol:                      Community:

[Edit]   [Delete]

---

**SNMP access settings**

| Community/User | Read access | Write access | Action |
|----------------|-------------|--------------|--------|
| [Add access]   |             |              |        |

[OK]

**Figure 6.59: Device SNMP Settings Screen**

The administrative user can use the screen shown in Figure 6.59 to configure the following:

- How the OnBoard appliance authenticates itself to a device when proxying SNMP functionality for the device
- How the users on the public side authenticate themselves to the OnBoard appliance, whether they are using SNMP functionality on the OnBoard appliance itself or SNMP functionality proxied from a device

## Configuring device SNMP settings

When the administrative user selects *Edit* on the Device SNMP settings screen, the following screen appears.

**Device sp1 SNMP settings**

Device alias: sp1  
 IP address: 172.20.0.2  
 OID:   
 SNMP version: v1   
 Community:

**Figure 6.60: Config-SNMP: Device SNMP Access Dialog With V1 or V2c Selected**

When v3 is selected, the following screen appears.

**Device sp1 SNMP settings**

Device alias: sp1  
 IP address: 172.20.0.2  
 OID:   
 SNMP version: v3   
 User name:   
 Auth method: MD5   
 Auth pass:   
 Encryption: DES   
 Crypt pass:

**Figure 6.61: Config-SNMP: Device SNMP Access Dialog With V3 Selected**

## Configuring SNMP device access settings

When the administrative user selects the *Add Access* button on the Device SNMP Settings screen, the SNMP access configuration dialog box appears.

The fields on the screen vary according to which SNMP protocol type is selected.

**To begin configuring SNMP for a device:**

1. Log into *the* Web Manager as an administrative user.
2. Select the *Config-SNMP* menu option.
3. Click the *SNMP configure* button for the desired device under the Servers SNMP configuration heading. The Device devicename SNMP settings dialog appears.

**To configure a device's SNMP settings:**

Perform this procedure to configure how the OnBoard appliance authenticates itself to the selected device when proxying SNMP functionality for the device.

1. Log into the Web Manager as an administrative user.
2. Select the *Config-SNMP* menu option.
3. Select a device to configure.
4. Click *Edit* under the Service Processor SNMP setting heading. The Device <devicename> SNMP settings dialog appears.
5. Enter the identifier for the object to be managed in the OID field.
6. Select a version from the SNMP version pull-down menu.
7. If either the v1 or v2c version is selected in step 6, enter a community name in the Community field.

-or-

If the v3 version is selected in step 6, do the following steps.

- a. Enter the username required for authentication in the User name field.
- b. Select an authentication method from the Auth method pull-down menu.
- c. Enter an optional authentication password in the Auth pass field.
- d. Select an encryption method from the Encryption pull-down menu.
- e. Enter an optional encryption password in the Crypt pass field.
- f. Click *OK*.

**To configure a device's SNMP access settings:**

Perform this procedure to configure how users on the public side authenticate themselves to the OnBoard appliance, whether they are using SNMP functionality on the OnBoard appliance itself or SNMP functionality proxied from the device.

1. Select a device to configure on the Config-SNMP page, as described under *To begin configuring SNMP for a device:* on page 164.
2. Click the *Add access* button under the SNMP access settings heading. The Device - *devicename*- SNMP access configuration screen appears.
3. Select a version from the SNMP version pull-down menu.



4. If either the v1 or v2c version is selected in step 3, do the following steps.
  - a. Enter a community name in the Community field.
  - b. Select a Source radio button, either Default or Use IP.
  - c. If *Use IP* is selected, enter a source IP address.
  - d. If a view has been configured, select a Read view and Write view from the Security level pull-down menus.
5. Click *OK*.
6. Click *Save and apply changes*.

#### **To configure users with SNMP v3:**

If the v3 version is selected in step 3, configure users as desired by clicking the Add user button. The User configuration dialog appears.

1. Click the *Add user* button. The User settings dialog appears.
2. Enter a username in the User name field.
3. Select an authentication method from the Auth method menu.
4. Enter an optional authentication password in the Auth pass field.
5. Select an encryption method from the Encryption menu.
6. Enter an optional encryption password in the Crypt pass field.
7. Click *OK*.
8. Click *Save and apply changes*.

#### **To configure views with SNMP v3:**

1. Click the *Edit views* button. The Views configuration dialog appears.
2. Click the *Add View* button. The SNMP view settings dialog appears.
3. Enter a name for the view in the View name field.
4. Enter an OID for the object to be viewed in the OID field.
5. If desired, enter a Mask to create a OID subtree.
6. If desired, exclude the defined OID subtree by selecting the *Exclude* option from the left menu.
7. Click *OK*.
8. Click *Save and apply changes*.

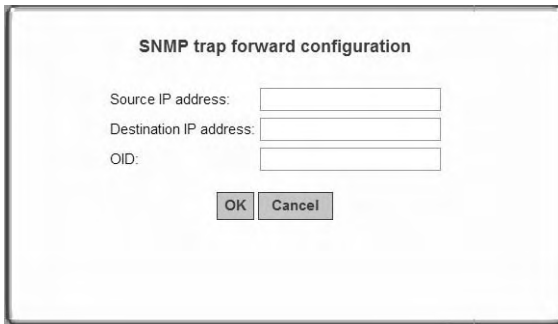
#### **To configure security with SNMP v3:**

1. Select a read view and write view from the No auth menus under the Read view and Write view columns.
2. Select a read view and write view from the Auth menus under the Read view and Write view columns.

3. Select a read view and write view from the Auth & crypt menus under the Read view and Write view columns.
4. Click *OK*.
5. Click *OK*.
6. Click *Save and apply changes*.

## Configuring SNMP trap forwarding for devices

Select *Add trap* on the Config-SNMP Configuration screen to access the Add Trap Forwarding screen.



The image shows a dialog box titled "SNMP trap forward configuration". It contains three input fields: "Source IP address:", "Destination IP address:", and "OID:". Below the input fields are two buttons: "OK" and "Cancel".

**Figure 6.62: Config-SNMP: Add Trap Forwarding**

Administrative users can use this screen to enable notifications about significant events occurring on connected devices to be sent from the OnBoard appliance to an SNMP management application, such as HP Openview, Novell NMS, IBM NetView or Sun Net Manager.

### To configure SNMP trap forwarding:

1. Log into the Web Manager as an administrative user.
2. Select the *Config-SNMP* menu option.
3. Click the *Add trap* button under the Trap forward configuration heading.
4. Enter an optional IP address in the Source IP address field.
5. Enter the IP address of the SNMP server to receive the trap in the Destination IP address field.
6. Enter the OID of the device in the OID field.
7. Click *OK*.
8. Click *Save and apply changes*.

## Configuring Logging of System Messages (Syslogs)

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.

See *Message Logging (With Syslog) on the OnBoard Appliance* on page 39 for more details.

## Syslog destination

The administrative user can use the *Config-Syslog* screen to tell the OnBoard appliance to send syslog messages to one or all of the following:

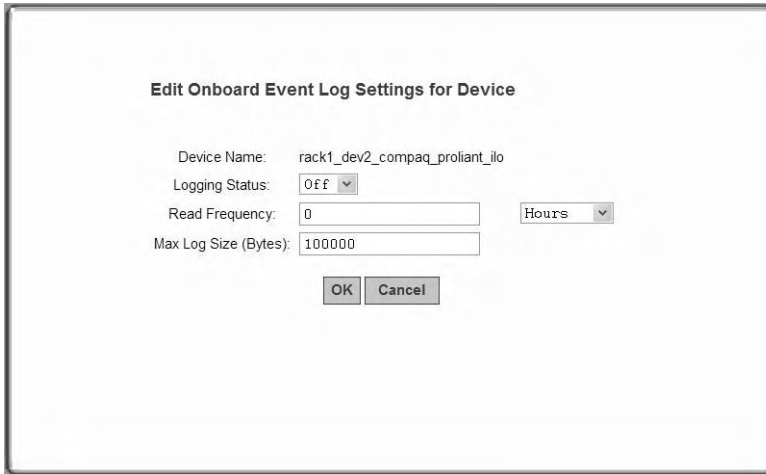
- Console
- Root user (if the root user is configured to receive syslog messages, make sure to configure an email address under Network-Outbound email)
- Syslog server

### To configure the Syslog destination and message filtering:

1. Log into the Web Manager as an administrative user.
2. Select the *Config-Syslog* menu option. The Syslog screen displays.
3. To configure messages to be sent to the console, click the *Console* checkbox.
4. To configure messages to be sent to the root user, click the *Root user* checkbox.
5. To configure messages to be sent to a syslog server, add a syslog server to the Syslog servers list by doing the following steps.
  - a. Enter a syslog server's IP address in the New syslog server field.
  - b. Click the *Add* button.
  - c. To add additional syslog servers, repeat steps a and b.
6. 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.
7. 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.
8. Click *Save and apply changes*.

## Configuring the Event Log Backend

When an administrative user selects the *Config-Event log backend* menu option, a screen appears with an entry for each configured device and an Edit button next to each device's entry. An administrative user can use the Config-Event log backend screen to configure event logging for connected service processors. Clicking an Edit button on the screen will bring up the Edit Dialog screen.



The screenshot shows a dialog box titled "Edit Onboard Event Log Settings for Device". It contains the following fields and controls:

- Device Name: rack1\_dev2\_compaq\_proliant\_ilo
- Logging Status: Off (dropdown menu)
- Read Frequency: 0 (text input field)
- Unit: Hours (dropdown menu)
- Max Log Size (Bytes): 100000 (text input field)
- Buttons: OK and Cancel

**Figure 6.63: Config-Event Log Backend: Edit Dialog**

### To configure system event logging for connected SPs:

1. Log into the Web Manager as an administrative user.
2. Select the *Config-Event log backend* menu option. The Event log backend profile screen appears.
3. Click the *Edit* button to edit event logging for a device. The Edit OnBoard appliance Event Log Settings for Device appears.
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 selects the *Config-Security profile* menu option, a screen appears that 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 *OnBoard Appliance Security Profiles* on page 30.

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.

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 appliance.

See Chapter 4 for the features in the Moderate security profile, the features in the Secured security profile and the features in the Open security profile.

The Moderate profile is the default option selected on the Security level menu.

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.

---

**NOTE:** If you select the secured profile, HTTP is disabled by the secured security profile. Follow the reminder at the bottom of the screen by making sure to notify all users that they must use HTTPS when bringing up the Web Manager.

---

### To select or customize the OnBoard appliance's security profile:

1. Log into the Web Manager as an administrative user.
1. Select the *Config-Security profile* menu option. The Security profile screen displays.
2. Click the *Proceed* button.
3. Select a security profile from the Security Level pull-down menu.
4. 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.
5. Click *OK*. The security profile confirmation screen appears.
6. Click *Save and apply changes*.

### To configure services:

When an administrative user selects the *Config-Services* menu option, the Config-Services screen appears with checkmarks next to the services that have been enabled by default. Enable or disable

any of the listed network services by clicking in the checkboxes next to the corresponding service and then clicking Save and apply changes to enable or disable any selections.

## Web Manager Network Menu Options

When an administrative user selects the *Network* top menu option, six options appear in the left menu, as shown in the following figure.

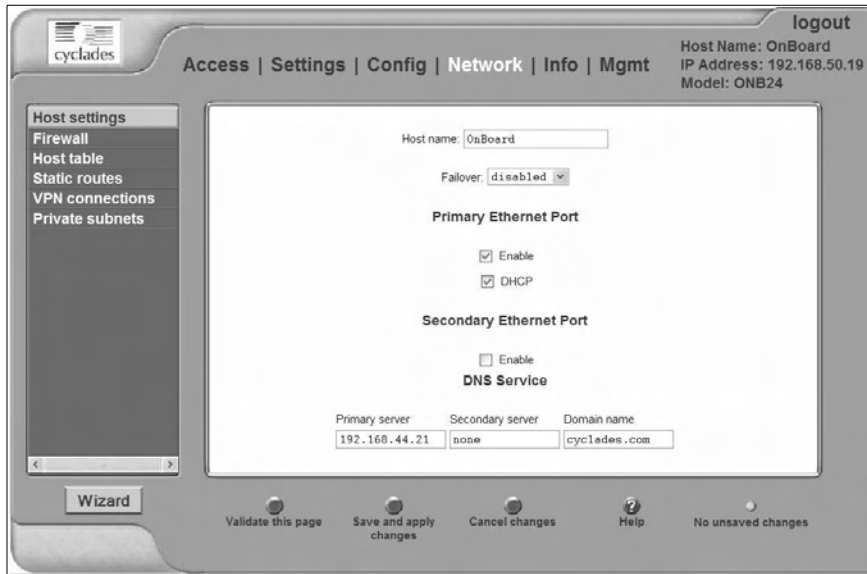


Figure 6.64: Network Menu Options

## Configuring network interfaces

When an administrative user clicks the *Network-Host settings* menu option, the following screen appears.

**Figure 6.65: Network-Host Settings Screen**

An administrative user can use this screen to configure the OnBoard appliance's network interfaces. The administrative user also can configure DNS for the OnBoard appliance by entering the DNS server and domain name information at the bottom of the screen.

The screen shown above allows an administrative user to set or change the parameters in the following table.

**Table 6.16: 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. Selecting disabled causes additional fields to display to allow configuration of one or both of the public Ethernet ports. |
| Host name            | Default: OnBoard                                                                                                                                                                                                                                                        |
| Primary DNS server   | IP address for a primary DNS server on the same subnet as the OnBoard appliance.                                                                                                                                                                                        |
| Secondary DNS server | IP address for an optional secondary DNS server on the same subnet as the OnBoard appliance.                                                                                                                                                                            |
| Domain name          | Domain name used on the domain name server (DNS).                                                                                                                                                                                                                       |

When configuring public Ethernet ports, be aware of the following:

- 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 appliance 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 appliance. When the *DHCP* checkbox is checked on any of the network interface screens, the DHCP server assigns the OnBoard appliance 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 use the Network-Static routes screen.

### Configuring failover

Figure 6.66 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.

The screenshot displays the Network-Host Settings configuration interface. At the top, the Host name is set to 'OnBoard'. Below this, the Failover option is set to 'enabled' via a dropdown menu. A section titled 'Failover Settings' contains a checkbox for 'DHCP' which is currently unchecked. Below the DHCP checkbox is a table of network parameters:

| IP Address     | Network Mask  | Gateway IP | Broadcast       | MTU  |
|----------------|---------------|------------|-----------------|------|
| 192.168.160.10 | 255.255.255.0 | none       | 192.168.160.255 | 1500 |

Below the network parameters is a section titled 'DNS Service' with three input fields: Primary server (192.168.44.21), Secondary server (none), and Domain name (cyclades.com).

**Figure 6.66: 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 6.66 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 Figure 6.67 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 screenshot shows the Network-Host Settings screen with the following configuration:

- Host name: OnBoard
- Failover: disabled
- Primary Ethernet Port**
  - Enable:
  - DHCP:
  - IP Address: 192.168.160.10
  - Network Mask: 255.255.255.0
  - Gateway IP: none
  - Broadcast: 192.168.160.255
  - MTU: 1500
- Secondary Ethernet Port**
  - Enable:
  - DHCP:
  - IP Address: [empty]
  - Network Mask: [empty]
  - Gateway IP: none
  - Broadcast: [empty]
  - MTU: 1500
- DNS Service**
  - Primary server: 192.168.44.21
  - Secondary server: none
  - Domain name: cycLades.com

**Figure 6.67: Network-Host Settings Screen, Both Interfaces Enabled and DHCP Disabled**

### To configure OnBoard appliance network interfaces:

1. Log into the Web Manager as an administrative user.
2. Select the *Network-Host settings* menu option.
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 appliance'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 packet filtering**

When an administrative user selects the *Network-Firewall* menu option, the following screen appears. The administrative user can use this screen to configure packet filtering.



**Figure 6.68: Network-Firewall Screen**

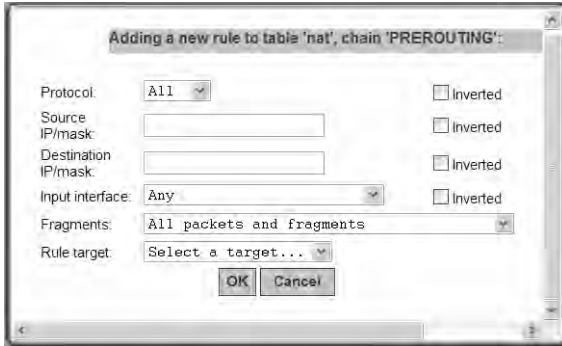
The Network-Firewall screen provides an interface to iptables. Using this screen, an administrative user can define rules for the built-in chains. Once rules have been administratively defined, they can be edited or deleted.

Figure 6.68 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 6.68 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 a Delete button appear next to the entry for each administrator-defined rule.

## Adding a rule

Clicking an Add new *table\_name chainname* rule button brings up a dialog like the one shown in Figure 6.69, which shows the dialog that appears when the administrative user clicks the Add new NAT prerouting rule button.



**Figure 6.69: Network-Firewall: Add Rule Dialog**

### To add a new packet filtering (firewall) rule:

1. Log into the Web Manager as an administrative user.
2. Select the *Network-Firewall* menu option.
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 *Save and apply changes..*

### To edit an administrator-added packet filtering (firewall) rule:

1. Log into the Web Manager as an administrative user.
2. Select the *Network-Firewall* menu option.
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* or *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 *Save and apply changes*.

## Configuring hosts

When an administrative user selects the *Network-Host table* menu option, the following screen appears.



Figure 6.70: Network-Host Table Screen

The following figure shows the dialog that appears when the administrative user clicks the *Add new host* button on the screen shown in Figure 6.70.



Figure 6.71: Network-Host Table: Add New Host Dialog

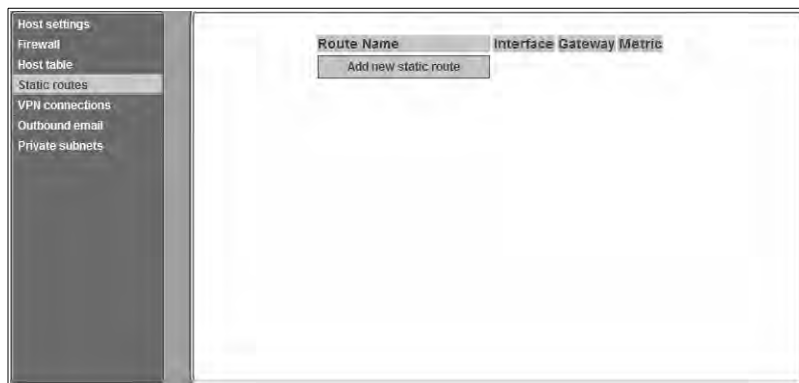
When adding a host, the administrative user must enter the information in the IP address and Name fields. Entering an alternative name in the Alias field is optional.

### To add a new host:

1. Log into the Web Manager as an administrative user.
2. Select the *Network-Host* menu option.
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 *Save and apply changes*.

## Configuring static routes

When an administrative user selects the *Network-Static routes* menu option, the following screen appears.



**Figure 6.72: 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.

**Table 6.17: 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 <i>networkIPaddress/mask_length</i> (also referred to as prefix/length).<br><b>NOTE:</b> To set a default route, go to Network-Host Settings. |
| Type               | Pull-down menu choices are Gateway or Interface.                                                                                                                                                                            |

**Table 6.17: Fields and Menus for Configuring Static Routes (Continued)**

| Field or Menu Name | Definition                                                                                                                                                                                                                                                                                                                                                                                                                 |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Interface/Gateway  | <ul style="list-style-type: none"> <li>• When Interface is selected from the Type menu, the Interface/Gateway menu choices are:               <ul style="list-style-type: none"> <li>• Public 1</li> <li>• Public 2</li> <li>• Failover</li> <li>• PCMCIA 1</li> <li>• PCMCIA 2</li> </ul> </li> <li>• When Gateway is selected from the Type menu, a field appears for entering the IP address of the gateway.</li> </ul> |
| Metric             | Enter the number of hops to the destination.                                                                                                                                                                                                                                                                                                                                                                               |

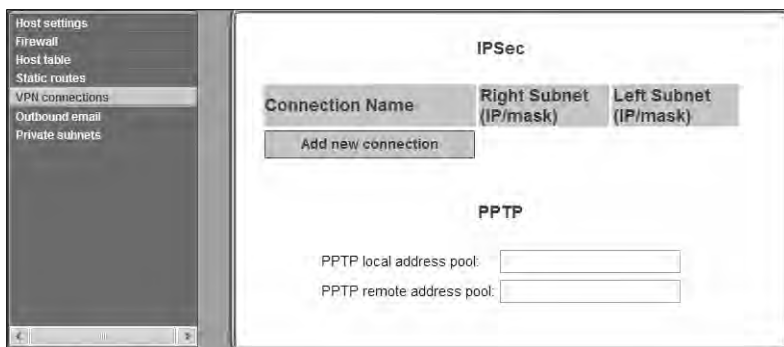
**To add a static route:**

1. Log into the Web Manager as an administrative user.
2. Select the *Network-Static routes* menu option.
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 *Save and apply changes*.

**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.

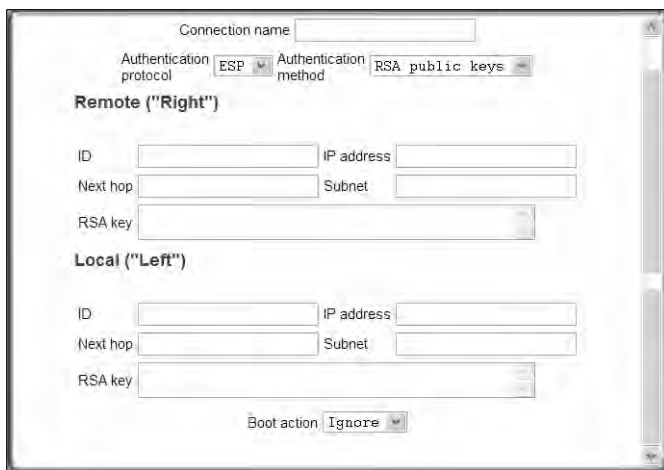
When an administrative user selects the *Network-VPN connections* menu option, the following screen appears.



**Figure 6.73: Network-VPN Connections Screen**

### 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 6.74: IPSec VPN Connection Configuration Dialog**

The administrative user can define multiple IPSec VPN connections.

#### To configure IPSec VPN:

1. Log into the Web Manager as an administrative user.
2. Select the *Network-VPN connections* menu option.
3. Click *Add new connection*.



4. The 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 performing the following steps.
  - a. Enter the name of the OnBoard appliance (left host) or the remote computer (right host) in the ID field.
  - b. Enter the IP address of the OnBoard appliance (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, perform one of the following steps.
  - a. When configuring the left host, generate the key for the OnBoard appliance 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*, *Add and route* or *Start* from the Boot Action pull-down menu.
12. Click *OK*.
13. Click *Save and apply changes*.

### Configuring PPTP VPN connections

The OnBoard appliance 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 appliance, the administrative user needs to fill in the PPTP fields in Figure 6.75 from the Network-VPN Connections Screen.

PPTP

PPTP local address pool:

PPTP remote address pool:

**Figure 6.75: PPTP VPN Connection Configuration Fields**

Table 6.18 describes the fields for configuring a PPTP profile. Specify a pool of addresses in the form 10.0.0.100-110.

**Table 6.18: Fields for Configuring a PPTP Profile**

| Field                    | Purpose                                                                                                                                         |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| PPTP local address pool  | Assign an OnBoard appliance IP address or range of addresses to be used whenever a user creates a PPTP VPN connection to the OnBoard appliance. |
| 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 appliance.             |

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.

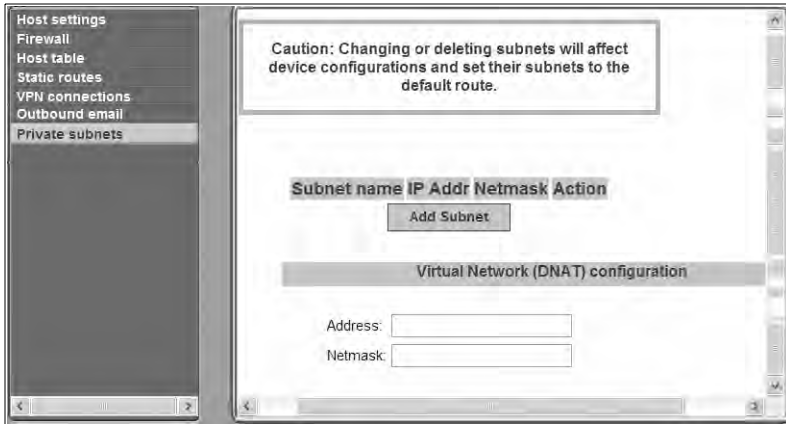
#### **To configure a PPTP VPN connection:**

1. Log into the Web Manager as an administrative user.
2. Select the *Network-VPN connections* menu option.
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 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 *Device Configuration* on page 230.

When an administrative user selects the *Network-Private subnets* menu option, the following screen appears.



**Figure 6.76: Network-Private Subnets Screen**

The administrator must define at least one subnet. In certain cases, the administrator may also need to define a virtual (DNAT) network.

### Adding private subnets

The administrator must define at least one subnet to enable devices that are connected to the OnBoard appliance's private Ethernet ports to communicate on the Internet via the OnBoard appliance's public IP address. Any number of private subnets may be configured.

---

**NOTE:** The OnBoard appliance attempts to reach a device that does not have a private subnet assigned by attempting to contact it through the OnBoard appliance's default route. Therefore, unless the OnBoard appliance 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 appliance. In almost all cases, devices are on the private side of the OnBoard appliance 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.

Subnets are defined as described in the following table.

**Table 6.19: 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 appliance. The OnBoard appliance 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 appliance derives the range of addresses in the subnet from the OnBoard appliance side IP address and the subnet mask. The OnBoard appliance uses the specified information to create a route to the subnet in the OnBoard appliance's routing table.

**Figure 6.77: Network-Private Subnets: Add Subnet Dialog**

The example in Figure 6.77 defines 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 should define a virtual network based on Destination Network Address Translation (DNAT) in the following cases:

- When multiple non-contiguous private subnets must be supported by a single network route (or, in the case of IPSec, a single tunnel) on the client for VPN or native IP access. This would be the case when connected devices are already configured using IP addresses from multiple address ranges and it is not feasible to change previously-defined device IP addresses
- When it is important to hide the addresses of the connected devices from users by the use of virtual IP addresses

**Table 6.20: Fields on the Private Subnet Virtual Network Configuration Dialog**

| Field   | Description                                                                                                                                                                                                                                          |
|---------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Address | IP address to assign to the OnBoard appliance 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 appliance that could be entered here. |

**Table 6.20: Fields on the Private Subnet Virtual Network Configuration Dialog (Continued)**

| Field   | Description                                                                                                                                     |
|---------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| 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.
2. Select the the *Network-Private subnets* menu option.
3. Click the *Add Subnet* button. The Private Subnet configuration dialog appears.
4. Enter a meaningful name for the private subnet in the Private subnet name field.
5. Enter an IP address for the OnBoard appliance within the private subnet's network address range in the Onboard side IP address field.
6. Enter a netmask for the private subnet in the Subnet netmask field.
7. Click *OK*.
8. Click *Save and apply changes*.

**To configure a virtual network:**

1. Log into the Web Manager as an administrative user.
2. Select the *Network-Private subnets* menu option.
3. Under Virtual Network (DNAT) configuration, enter a virtual IP address to assign to the OnBoard appliance from the virtual network's address range in the Address field.
4. Enter the netmask for the virtual network in the Netmask field.
5. Click *Save and apply changes*.

## Web Manager Info Menu Options

Figure 6.78 shows the three options that appear in the left menu when an administrative user selects the *Info* top menu option.



**Figure 6.78: Info Menu Options**

Table 6.21 lists the sections that describe the options that appear when an administrative user clicks *Info*.

**Table 6.21: Options Under Info**

| Option             | Where Described                                                     |
|--------------------|---------------------------------------------------------------------|
| Session status     | <i>Viewing status information about active sessions on page 187</i> |
| System Information | <i>Viewing system information on page 188</i>                       |
| Detected devices   | <i>Viewing information about detected devices on page 188</i>       |

## Viewing status information about active sessions

When an administrative user selects the *Info-Session status* menu option, the following screen appears.



Figure 6.79: Info-Session Status Screen

Table 6.22: Information on the Info-Session Status Screen

| Heading Name | Description                                                                             |
|--------------|-----------------------------------------------------------------------------------------|
| Alias        | Name/alias configured for the device on the OnBoard appliance                           |
| Command      | Device management command being used                                                    |
| User Name    | Name of the user account accessing the device                                           |
| Port         | Number of the OnBoard appliance private port through which the device is being detected |

**NOTE:** More than one device may be accessed through a single OnBoard appliance 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 selects the *Info-System information* menu option, the following screen appears.

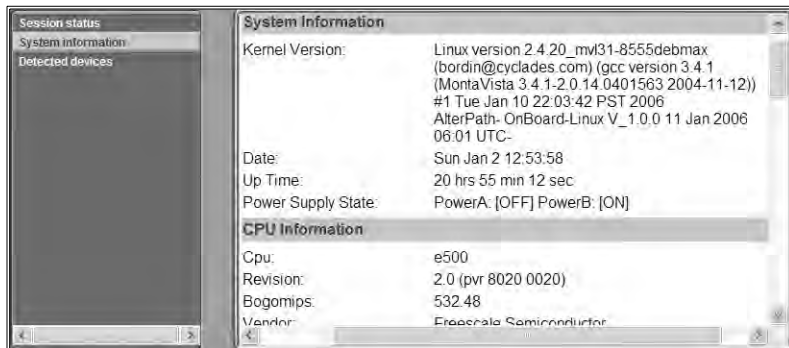


Figure 6.80: Info-System Information Screen

## Viewing information about detected devices

When an administrative user selected the *Info-Detected devices* menu option, the following screen appears.

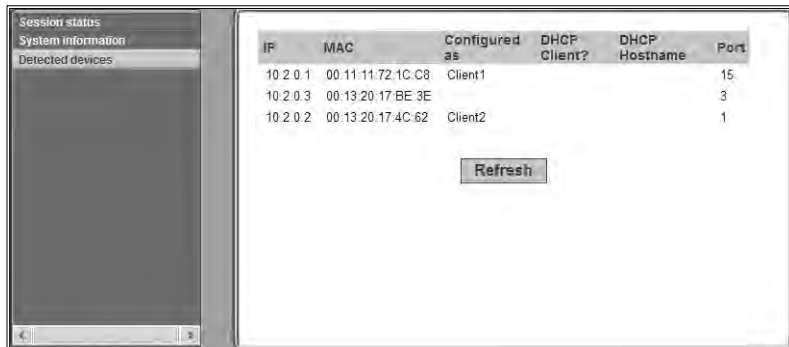


Figure 6.81: Info-Detected Devices Screen

Table 6.23: 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 appliance. |

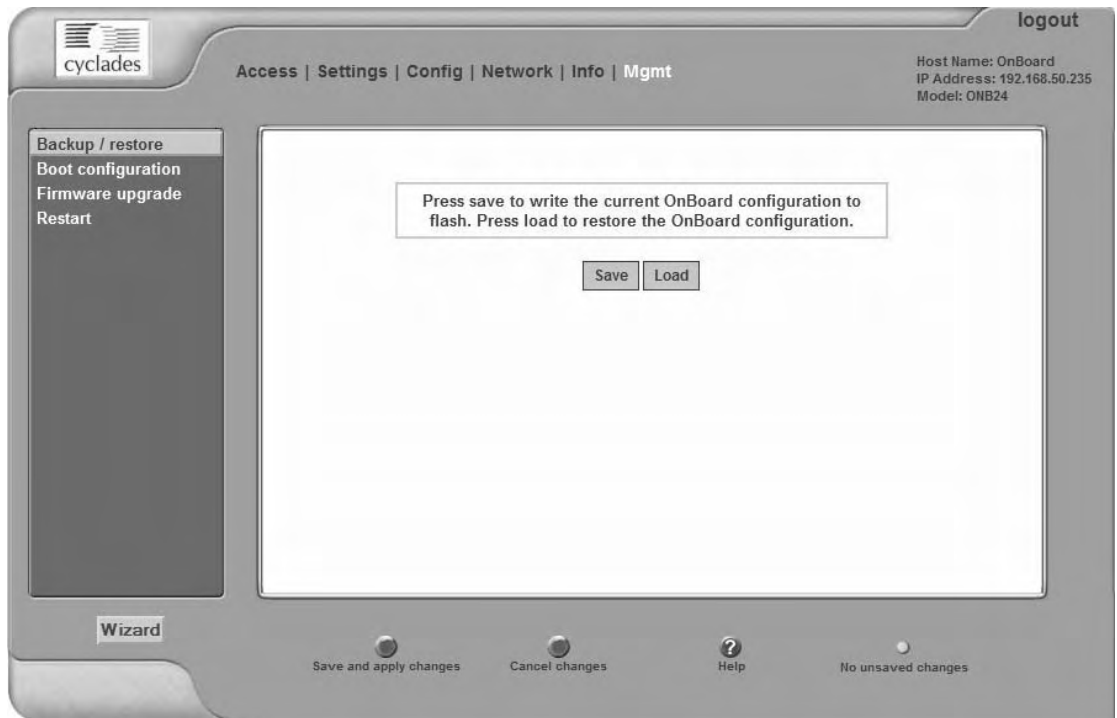


**Table 6.23: Information on the Info-Detected Devices Screen (Continued)**

| Heading Name  | Description                                                                                                                                                                                                                                |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DHCP Client?  | If the OnBoard appliance DHCP server is enabled and if the detected device obtained a dynamically allocated (instead of fixed) IP address from the OnBoard appliance, YES appears in this column. In all other cases, the column is empty. |
| DHCP Hostname | If a DHCP client sends a hostname as part of its DHCP request to the OnBoard appliance, and if the assigned address is not reserved, the DHCP hostname provided by the client appears in this column.                                      |
| Port          | The number of the OnBoard appliance private port through which the device is being detected.                                                                                                                                               |

## Web Manager Mgmt Menu Options

Figure 6.82 shows the four left menu options that appear when an administrative user selects the *Mgmt* (Management) top menu option.

**Figure 6.82: Mgmt Options**

## Backing up or restoring configuration files

When an administrative user selects the *Mgmt-Backup/restore* menu option, the following screen appears.



**Figure 6.83: Mgmt-Backup/restore Screen**

Clicking the *Save* button backs up the current state of the Onboard configuration files in a compressed backup file in Flash memory and overwrites any previous configuration backup file.

Clicking the *Load* button overwrites the current state of the configuration files with the last backup copy that was made.

### To back up configuration files:

1. Bring up the Web Manager and log in.
2. Select the *Mgmt-Backup/restore* menu option.
3. Click the *Save* button to back up the current state of the configuration files.
4. Click *Save and apply changes*.

### To restore backed-up configuration files:

1. Bring up the Web Manager and log in.
2. Select the *Mgmt-Backup/restore* menu option.
3. Click the *Restore* button to restore any previously-saved configuration files.
4. Click *Save and apply changes*.

## Upgrading OnBoard appliance firmware

When an administrative user selects the *Mgmt-Firmware upgrade* menu option, the following screen appears.

The upgrade will only be performed if the "Upgrade Now" button is pressed.  
See Help for more details.

**Image source**

FTP site (IP address or hostname):   Use passive mode FTP

Username:

Password:

Image file (path and filename):

**Installation parameters**

**The image will be installed into the non-active partition** – the current image will be kept as a backup.  
The **current configuration** will be copied and used for the new image.  
**The installed image will automatically be made active** – it will be used at the next boot.

**Figure 6.84: Mgmt-Firmware Upgrade Screen**

An administrative user can use the screen to upgrade the OnBoard appliance's operating system kernel and applications, which are collectively referred to as firmware in Cyclades management interfaces.

The current configuration is used after the upgrade. The installed software is used at the next boot, which should be performed after the upgrade completes.

### 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 appliance. Table 6.23 describes the information you need to supply on the form.

**Table 6.24: Firmware Upgrade Screen Fields**

| Field/Menu Name | Definition                                                                                                                                                                                             |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| FTP site        | The DNS name or IP 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. |
| 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.                                                                                   |

**Table 6.24: Firmware Upgrade Screen Fields**

| Field/Menu Name                | Definition                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Image file (path and filename) | The pathname of the software image file on the ftp server.<br>On the Cyclades ftp server, the directory is under /pub/cyclades/alterpath/onboard/released/V_version_number/zImage_onb_NNN, where version_number is 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 appliance. |

**To download OnBoard appliance firmware:**

- From a local FTP or TFTP server, log into a local ftp server as root.
- Change to the directory into which the software needs to be downloaded.

```
cd /tmp
```
- 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):
```
- 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>
```
- 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 Apr 06 2006 V_1.1.0
drwxr-xr-x 2 1006 100 4096 Aug 06 2006 V_3.0.0
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\_3.0.0.

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. Enter 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
```

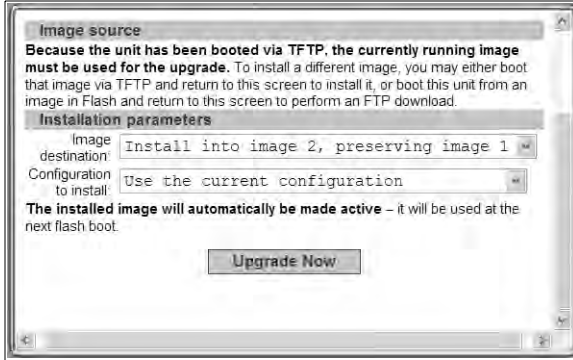
8. After the download completes, end the ftp connection, and verify the presence of the zImage\_onb\_110.bin and zImage\_onb\_110.md5 files on the local server.

```
ftp> bye
221 Goodbye.
ls
zImage_onb_110.bin
zImage_onb_110.md5
```

9. Log out from the console session and go to *To upgrade the OnBoard appliance firmware:* on page 194.

## Special considerations if the last boot was a network boot

Figure 6.85 shows the message that appears if the OnBoard appliance was last booted over the network from a TFTP server.



**Figure 6.85: Mgmt-Firmware Upgrade Screen With Net Boot Message**

Click the *Upgrade Now* button to write the currently-running image from the RAM memory into the Flash memory.

For more details about how images are stored in the OnBoard appliance and about configuration file backups, see *Advanced Boot and Backup Configuration*.

See Table 6.24 on page 191 if needed for the values to supply in the fields. To upgrade using an image booted over the network from a TFTP server, boot the OnBoard appliance from a TFTP server before starting the following procedure.

### To upgrade the OnBoard appliance firmware:

1. Log into the Web Manager as an administrative user.
2. Select the *Mgmt-Firmware upgrade* menu option. To upgrade from an image obtained from a tftp server after a network boot, go to step 4. To upgrade from an ftp server, continue to step 3.
3. To upgrade using an image from an ftp server, perform the following steps:
  - a. Enter the IP address or DNS name of the ftp server in the FTP site field.
  - b. If desired, check the checkbox next to *Use passive mode FTP*.
  - c. Enter the username for the ftp site in the Username field.
  - d. Enter the password required for accessing the ftp site in the Password field.
  - e. Enter the pathname of the software image file on the ftp server in the Image file field.
4. Click the *Upgrade Now* button.
5. When the download completes, select the *Mgmt-Restart* menu option and restart the appliance.

## Restarting the OnBoard appliance

When an administrative user selects the *Mgmt-Restart* menu option, the following screen appears.



**Figure 6.86: Mgmt-Restart Screen**

### To restart the OnBoard appliance:

1. Log into the Web Manager as an administrative user.
2. Select the *Mgmt-Restart* menu option.
3. Click the *Restart* button.





## Using the *cycli* Utility

The following sections describe how administrators (root and any administrative user) can use the *cycli* configuration utility.

- *cycli* Utility Overview on page 197
- Execution Modes on page 198
- Command line mode on page 198
- Interactive mode on page 198
- Batch mode on page 198
- *cycli* Options on page 199
- *cycli* Parameters and Arguments on page 199
- Entering a command in interactive mode on page 200
- Entering a command in command code on page 201
- Entering a command in batch mode on page 201
- Autocompletion on page 202
- *cycli* Commands on page 204
- Summary of How to Configure the Top Level Parameters on page 216

### **cycli** Utility Overview

An administrator can configure the OnBoard appliance using the *cycli* utility. Only one administrator can be logged into the OnBoard appliance at a time. While in the *cycli* utility, an administrator can escape to the shell and when finished can return to the *cycli* utility.

Administrators often prefer using the *cycli* utility 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 appliance with 40 private Ethernet ports, configuring all the SPs one by one could be tedious and prone to error, so scripting the configuration of multiple SPs 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 204) that act on parameters nested in a format called the CLI parameter tree. Some parameters require arguments when the parameters are entered with some commands.

---

**NOTE:** This section describes the `cycli` commands 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 a command line mode, batch mode and interactive mode.

### Command line mode

Command line mode refers to when the `cycli` utility is invoked on the Linux command line with options, commands, 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.

When invoked without commands, `cycli` enters interactive mode; see *Interactive mode*. When the `cycli` utility is invoked with the `-f` file option or is invoked from a script, the commands are executed in batch mode from the specified file or script.

### 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.

### 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 be 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.

## cycli Options

Administrators can invoke the cycli command with a number of different options shown in the following table.

**Table 7.1: cycli Utility Options**

| Option      | Description                                                                                                                             |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| -l          | 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 time-out | Sets the idle time-out in minutes. Default is 10 minutes.                                                                               |
| -T          | Disables idle time-out (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 appliance CLI configuration options are organized in a hierarchy called a parameter tree. You can use the get, show and list commands to show parameters. You can also use the get command to show the values of individual parameters at the end of a branch.

The following diagram illustrates one parameter in the OnBoard appliance cycli parameter tree. As shown in the example in Figure 7.1, 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.

```

network
 interface
 failover

```

**Figure 7.1: 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 the following command:

```
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 containing 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 7.1, 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 code

Based on the branch in Figure 7.1, 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 7.1, 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 example.

```
[root@onboard /]# chmod 777 scriptname1
[root@onboard /]# ./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 /]# chmod 777 scriptname2
[root@onboard /]# ./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 /]# 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.

## Examples

```
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>
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>
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 set using the set command.



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 (as in: `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.

You must add parameters in a prescribed order. For example, because an 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.

### **Synopsis**

```
add parameter(s) value(s)
```

## Examples

```
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
```

## Parameters

The following table shows the parameters that can be added using the add command. When a parameter is shown in the Parameter Level 2 column, the Parameter Level 1 and Parameter Level 2 parameters must be entered with the add command.

**Table 7.2: Parameters That Work With the `cycli add` Command**

| Parameter Level 1 | Parameter Level 2 | Configures                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-------------------|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| group             |                   | Add a group to the list of local groups: add group groupname. The group name is automatically assigned a gid.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| ipsec             | conn              | Adds a VPN IPsec connection: add ipsec conn connection_name. Then use the set command to set the following for the left host: a left host IP address [left IPAddress], an optional alias for the left host [leftid alias], an optional RSA key [leftsasigkey key], an optional_subnet IP address [leftsubnet IPAddress], an optional next hop IP address [leftnexthop IPAddress]. Use the set command to set the following for the right host: a right host IP address [right IPAddress], an optional alias for the right host [rightid alias], an optional RSA key [rightsasigkey key], an optional subnet IP address [rightsubnet IPAddress], an optional next hop IP address [rightnexthop IPAddress]. |

**Table 7.2: Parameters That Work With the cycli add Command (Continued)**

| Parameter Level 1 | Parameter Level 2 | Configures                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-------------------|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                   | key               | Adds a shared key: add ipsec key key_name. Then use the set command to set the key [set key_name key]. The key can be in hexadecimal (with the 0x prefix followed by any of: a-f, A-F, 0-9), in base 64 (with the 0s prefix followed by any base 64 number using a-z, A-Z, +, or \); or a text string (entered with the 0t prefix followed by text):                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| iptables          | nat filter        | Add chainname to the list of chains: add iptables nat filter chainname. 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. Then use the set command to set filtering policies for each rule, by optionally specifying one or more of the following: a destination IP, [destination IPAddress]; whether to invert the destination IP [inv]; a source IP address [source IPAddress] whether to invert the source IP address [inv]; a protocol [tcp, udp, icmp, all or a protocol number], whether to invert the protocol [inv]; for protocol tcp or udp, the destination port [dport]; source port [sport]; whether to invert the protocol [inv]; an input interface [in-interface]; whether to invert the in-interface [inv]; an output interface [out-interface]; whether to invert the out-interface [inv]; whether to allow fragments [fragment yes] or to disallow all fragments [fragment no]; whether to invert the fragment yes   no [inv]; a target action [target action]. For NAT and filter, the following target actions are defined: DROP, ACCEPT, REJECT or chainname. For NAT, the following additional target actions are defined: DNAT to change the destination address [DNAT to-destination IPAddress]; and SNAT, to change the source IP [SNAT to-source IPAddress]. |
| network           | hosts             | Add an IP address for a host: add network hosts IPAddress. Then use the set command to set the following for the host: a hostname [name], an optional alias [alias].                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|                   | st_routes         | Add to the list of static route targets a subnet or host (networks in the form 1.2.3.4/255.255.0.0 or host IPs): add network st_routes network_IPAddress/netmask   host_IPAddress.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| notifications     |                   | Add a notification using any name add notifications notification_name. Then use the set command to set the trigger specifying the format used for triggers in the /etc/syslog.ng file [trigger trigger_string]; a notification type, one of SNMP, SMS or MAIL [type SNMP SMS MAIL].                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

**Table 7.2: Parameters That Work With the `cycli add` Command (Continued)**

| Parameter Level 1 | Parameter Level 2 | Configures                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-------------------|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                   |                   | If MAIL is set, then use set notifications MAIL with the recipient email address [to email_address]; sender email address [from email_address]; Subject: line in quotes [subjectsubject of the notification email]; email message body in quotes [body body of the email message]; mail server IP address [mail_server IP_address].                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|                   |                   | If SNMP is set, use set notifications snmptrap with an OID [oid OID]; trap number [trapnumber number]; community name [community community_name]; server IP address [server IPAddress]; message body in quotes [body body of the email message].                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|                   |                   | If SMS is set, use set notifications pager with an pager number [number pager_number], message body in quotes [body body of the pager message]; username [user username]; server IP address [server IPAddress]; port number [port number].                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| onboard           | server            | Add a managed device (SP, server, or device): add server device_name. Also use the set command to set the type: drac, rsa-II, ilo, ipmi1_5 [type device_type], devconsole, custom1, custom2, custom3; authentication type: kerberos, kerberosdownlocal, ldap, ldapdownlocal, local, localnis, localradius, localtacplus, nis, nisdownlocal, nislocal, none, radius, radiusdownlocal, radiuslocal, smb, smbdownlocal, tacplus, tacplusdownlocal, tacpluslocal [authtype device_type]; the IP address for the device [ip   local_ip IP_address]; the device's netmask [netmask netmask]; if drac type is set, enter the DRAC console port ID, either com1 or com2 [drac_console_port com1   com2]; the login name [login username]; the user's password [password password]; a short description for the server in quotes [description device description]; enable or disable event logging [eventlog enable yes   no].<br>When eventlog is enabled, use the set command to set the frequency for logging in hours [frequency hours]; the maximum log size in bytes [maxlogsize size]. |
|                   | user group        | Add the name of a user or group authorized to access the device: add onboard user username   group groupname.<br>Add a device for an existing user or group when the device_name has been added as described under onboard server: add onboard user   group device_name. Then use the set command to set permissions for sensors, power, sel, spconsole, console, kvm, vpn, specifying either yes or no for each.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

**Table 7.2: Parameters That Work With the cycli add Command (Continued)**

| Parameter Level 1 | Parameter Level 2         | Configures                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-------------------|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| snmpd             | rwcommunity   rocommunity | Add a read-write community [rwcommunity] or a read-only community [rocommunity]: add snmpd rwcommunity   rocommunity community_name. Then use the set command to set the source IP [source] and OID [oid].                                                                                                                                                                                                                                                            |
|                   | rwuser   rouser           | Add a read-write user [rwuser] or a read-only user [rouser]: add snmpd rwuser   rouser user_name. Then use the set command to set the user level [level noauth   auth] and OID [oid].                                                                                                                                                                                                                                                                                 |
|                   | user                      | Add a user: add snmpd user user_name. Then use the set command to set the common method snmpd, proxy, or host [common]; the authentication method, MD5 or SHA [authmethod] and authentication pass phrase, must be greater than eight characters [authpassphrase]; encryption method, must be DES [cryptmethod]; encryption pass phrase, must be greater than eight characters [cryptpassphrase].                                                                     |
|                   | group                     | Adds a group: add snmpd group group_name. Then use the set command to set the security model: v1, v2c, or usm [sec_model] and security name [sec_name].                                                                                                                                                                                                                                                                                                               |
|                   | view                      | Adds a view: add snmpd view view_name. Also use the set command to set the policy as included or excluded [incl_excl included   excluded], [subtree], [mask].                                                                                                                                                                                                                                                                                                         |
|                   | access                    | Adds an access type. add snmpd access_type. Also use the set command to set the [context], security model: v1, v2c, or usm [sec_model v1   v2   usm], security level [sec_level], [match], [read write notif].                                                                                                                                                                                                                                                        |
|                   | proxy                     | Adds a snmpd view. Also use the set command to set common level [common snmpd proxy[\$i]-Cn], proxy version [version snmpd proxy[\$i]-Cn], a community or a user [community user]; OID [oid], security level [sec_level snmpd proxy[\$i]-Cn]; the location of the system, syslocation and contact person, syscontact [syscontact   syslocation].                                                                                                                      |
| syslog            | destination               | Adds a destination name for syslog messages: add syslog destination server_name. Also use the set command to enable or disable the destination [enable yes no]; set a destination type, one of tcp, udp, or file [type tcp   udp   file]; set a valid username as the owner of the tty [usertty username]; set an IP address for the destination [tcp udp IP_address]; set a destination filename [file filename]; set a named pipe as a destination [pipe pipename]. |

**Table 7.2: Parameters That Work With the `cycli add` Command (Continued)**

| Parameter Level 1 | Parameter Level 2                                                                                                                             | Configures                                                                                                                                                                                                                                                                                                                                                                                                 |
|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| user              | <b>NOTE:</b> Do not use. The correct way to add a user using the <code>cycli</code> is as an onboard user, as in: <b>add onboard user joe</b> | Add a user or users to the list of local users; add user username. Also use the <code>set</code> command to set the password [passwd password], user ID [uid UID], group ID [gid GID], group name [group groupname], identifying string for the user in quotes [gecos Identifying string for the user name], home directory [home directory_pathname], user type, regular or admin [type regular   admin]. |

## 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.

### Synopsis

```
cd [parameter(s)]
```

### Examples

```
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 are not updated, and your changes will be lost after the next reboot.

---

### Synopsis

```
commit
```

## 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.

### Synopsis

```
delete parameter(s)
```

Some parameters cannot be deleted. Parameters that can be added can be deleted.

### Examples

```
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
```

## 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.

### Synopsis

```
get | show parameter(s)
```

### Examples

```
cli> get network hostname
anchovy
cli> show network resolv domain
```

avocent.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.

```
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 appliance before any configuration has been done.

```
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 211), 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.

### Synopsis

```
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.

### Synopsis

quit

### 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.

### Synopsis

```
rename parameter(s) value(s)
```

### Examples

```
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.

**Synopsis**

```
revert
```

**Examples**

```
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.

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.

**Synopsis**

```
set parameter(s) value(s)
```

**Examples**

```
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
```

**shell**

Escape to shell. This command is only available to root.

**Synopsis**

shell

**Examples**

```
cli> shell
[root@onboard root]# whoami
root
[root@onboard root]# logout
cli>
```

**version**

Displays the current `cycli` version.

**Synopsis**

version

**Examples**

```
cli> version
OnBoard CLI 2.0 (2005-06-16T13:47+1000)
```

## Summary of How to Configure the Top Level Parameters

This section provides a brief overview of how to configure the top level parameters.

Typing any of the commands such as `add` or `set` then pressing **Tab Tab** 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
```

Table 7.3 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 7.3: Top Level cycli Parameters With Set or Add Commands**

| Parameter | Command                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| auth      | <ul style="list-style-type: none"> <li>Use the set command to set an authentication type for logins to the OnBoard appliance (set auth type authtype).</li> <li>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).</li> </ul>                                                                                                                                                                                                        |
| auxport   | <ul style="list-style-type: none"> <li>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).</li> </ul>                                                                                                                                                                                                                                   |
| bootconf  | Use the set command to configure boot configuration (set bootcon 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 (set cards cardtype Tab Tab shows the configuration parameters to set).                                                                                                                                                                                                                                                                                                                                                                                             |
| group     | Use the add command to add a group (add group groupname). A GID is automatically set.<br>Use the set command to configure the group members (set group groupname users.<br>username[,username2,...,usernameN).                                                                                                                                                                                                                                                                                                                                           |
| httpd     | Use the set command to configure HTTP/HTTPS services (set httpd http Tab Tab shows the configuration parameters to set).                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| ipdu      | <ul style="list-style-type: none"> <li>Use the set command to configure an IPDU (set ipdu s1 Tab Tab shows the configuration parameters to set).</li> <li>Use the set command to configure the outlets (set ipdu s1 Tab Tab shows the configuration parameters to set).</li> <li>Use the add command to add users who can configure outlets (add ipdu s1 users username).</li> <li>Use the set command to configure which outlets each user can manage (set ipdu s1 users username <b>Tab Tab</b> shows the configuration parameters to set).</li> </ul> |

**Table 7.3: Top Level cycli Parameters With Set or Add Commands (Continued)**

| Parameter               | Command                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ipsec conn              | <ul style="list-style-type: none"> <li>Use the add command to add a VPN IPsec connection name (add ipsec conn connectionname).</li> <li>Use the set command to configure the connection parameters (set ipsec conn connection_name <b>Tab Tab</b> shows the configuration parameters to set).</li> </ul>                                                                                                                                                                                                                 |
| iptables [filter   nat] | <p>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.</p> <ul style="list-style-type: none"> <li>Use the add command to add a chain of type filter or nat (add iptables [filter   nat] connectionname).</li> <li>Use the set command to configure the parameters (set iptables [filter   nat] <b>Tab Tab</b> shows the configuration parameters to set).</li> </ul> |
| network hostname        | Use the set command to configure the OnBoard appliance hostname (set network hostname OnBoard_hostname).                                                                                                                                                                                                                                                                                                                                                                                                                 |
| network hosts           | <ul style="list-style-type: none"> <li>Use the add command to add a host to the hosts table (add network hosts IP_address).</li> <li>Use the set command to configure the host (set network hosts IP_address <b>Tab Tab</b> shows the parameters to set).</li> </ul>                                                                                                                                                                                                                                                     |
| network interface       | Use the set command to configure one of the network interfaces (set network interface <b>Tab Tab</b> lists the interfaces to configure; set network interface interface_name <b>Tab Tab</b> lists the parameters to configure).                                                                                                                                                                                                                                                                                          |
| network ipv4            | Use the set command to configure ipv4 (set network ipv4 <b>Tab Tab</b> lists the parameters to configure).                                                                                                                                                                                                                                                                                                                                                                                                               |
| network resolv          | Use the set command to configure DNS (set network resolv <b>Tab Tab</b> lists the parameters to configure).                                                                                                                                                                                                                                                                                                                                                                                                              |
| network smtp            | Use the set command to configure email notifications to be sent to root (set network smtp <b>Tab Tab</b> lists the parameters to configure).                                                                                                                                                                                                                                                                                                                                                                             |
| network st_routes       | <ul style="list-style-type: none"> <li>Use the add command to add a static route to the routing table (add network st_routes IP_address).</li> <li>Use the set command to configure the static route (set network st_routes IP_address <b>Tab Tab</b> shows the parameters to set).</li> </ul>                                                                                                                                                                                                                           |

**Table 7.3: Top Level cycli Parameters With Set or Add Commands (Continued)**

| Parameter                                      | Command                                                                                                                                                                                                                                                                 |
|------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| notifications                                  | <ul style="list-style-type: none"> <li>Use the add command to add a notification (add notifications name).</li> <li>Use the set command to configure the parameters (set notifications name <b>Tab Tab</b> shows the parameters to set).</li> </ul>                     |
| 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 default databuf                 | Use the set command to configure the default for data buffering (set onboard global default databuf [yes   no]).                                                                                                                                                        |
| 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 <b>no</b> (set onboard global security override_authorizations [yes   no]).                                                                    |
| onboard global sort server                     | Use the set command to configure the sort method for the names of devices, either alphabetical or no sorting. By default, device names appear in the order they were configured (set onboard global sort server [alpha   none]).                                        |
| onboard global strict subnet                   | Use the set command to configure whether or not sanity checks are made for the subnet IP and netmasks. If set to no, overlapping subnets are allowed. (set onboard global strict subnet [yes   no]).                                                                    |
| onboard global strict uniqip                   | Use the set command to configure whether or not sanity checks are made to ensure that the real IP assigned to a device is unique. (set onboard global strict uniqip [yes   no]).                                                                                        |
| onboard group                                  | <ul style="list-style-type: none"> <li>Use the add com.mand to configure an onboard group (add onboard group groupname).</li> <li>Use the set command to configure the parameters (set onboard group servername <b>Tab Tab</b> shows the parameters to set).</li> </ul> |

**Table 7.3: Top Level cycli Parameters With Set or Add Commands (Continued)**

| Parameter      | Command                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| onboard server | <ul style="list-style-type: none"> <li>Use the add command to configure a device (add onboard server servername)</li> <li>Use the set command to configure the parameters (set onboard server servername <b>Tab Tab</b> shows the parameters to set). For example, set onboard server servername databuf [yes no default] configures whether data buffering is done according to the global setting or not.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                    |
| onboard user   | <ul style="list-style-type: none"> <li>Use the add onboard user command to configure a user (add onboard user username).</li> <li>Use the set user command to configure the normal Linux user's parameters such as passwd (set user username <b>Tab Tab</b> shows the parameters to set).</li> <li>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).</li> <li>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 <b>Tab Tab</b> shows the device management actions to set by specifying yes or no for each).</li> </ul> |
| pptpd          | Use the set pptpd command to configure PPTP (set pptpd <b>Tab Tab</b> shows the parameters to set).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| profile        | Use the set profile command to select the security profile (set profile <b>Tab Tab</b> shows the parameters to set).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| sensoralarm    | <ul style="list-style-type: none"> <li>Use the add sensoralarm command to configure a sensor alarm (add sensoralarm alarm_ID).</li> <li>Use the set sensoralarm command to configure the parameters (set sensoralarm alarm_ID <b>Tab Tab</b> shows the parameters to set). Use the name of a sensor on the device in quotes (such as Sys Fan 1) and an appropriate range if you specify inside or outside.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                     |
| service        | Use the set service command to enable or disable any service (set service <b>Tab Tab</b> shows the services to enable or disable by specifying enable yes or enable no for each).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |



**Table 7.3: Top Level cycli Parameters With Set or Add Commands (Continued)**

| Parameter                                      | Command                                                                                                                                                                                                                                                                                                         |
|------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| snmpd [access   com2sec   group   user   view] | <ul style="list-style-type: none"> <li>Use the add snmpd command to add access, com2sec, group, user and view (add snmpd [access   com2sec   group   user   view]).</li> <li>Use the set snmpd command to configure the parameters (set snmpd parameter <b>Tab Tab</b> shows the parameters to set).</li> </ul> |
| sshd                                           | Use the set sshd command to enable or disable SSHD (set sshd <b>Tab Tab</b> shows the parameters to set).                                                                                                                                                                                                       |
| syslog                                         | Use the set syslog command to specify a syslog server (set syslog <b>Tab Tab</b> shows the parameters to set).                                                                                                                                                                                                  |
| timezone                                       | Use the set timezone command to specify the timezone (set timezone <b>Tab Tab</b> shows the parameters to set).                                                                                                                                                                                                 |
| user                                           | <ul style="list-style-type: none"> <li>Do not use this command to add a user. Use add onboard user username first.</li> <li>Use the set user command to configure the normal Linux user's parameters such as the passwd (set user username <b>Tab Tab</b> shows the parameters to set).</li> </ul>              |
| web                                            | Use the set web command to specify a user-accessible server where the help files have been downloaded (set web <b>Tab Tab</b> shows the parameter to set). The default is <a href="http://www.cyclades.com/online-help/onb/v_1.0.0/">http://www.cyclades.com/online-help/onb/v_1.0.0/</a> .                     |



## APPENDICES

# Appendix A: Troubleshooting

## Network failure

This section summarizes the options for connecting to the OnBoard appliance for troubleshooting in the event of an IP network failure.

Remote OnBoard appliance administrators can connect to the OnBoard appliance in case of network failure in any of the following ways:

- By bringing up the Web Manager or logging into the OnBoard appliance'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 appliance
  - A modem on a PCMCIA modem card optionally installed in the OnBoard appliance
- By logging into the OnBoard appliance's console after establishing a dial-in connection from a terminal emulation program to an external modem optionally connected to the OnBoard appliance.

Local OnBoard appliance administrators can connect to the OnBoard appliance by logging into the Linux command line through a terminal or workstation that is connected to the OnBoard appliance's console port.

All of these connection methods must be previously configured as described elsewhere in this manual. For example, to make it possible to dial in if the network connection becomes unavailable, a modem must be installed and configured.

## Login failure

If no one can log into the OnBoard appliance, you can perform the following procedure to reset the root or admin user's password. This procedure would be needed, for example, if an attempt to log into 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 login failure:

1. Boot the OnBoard appliance in the U-Boot monitor mode.

See *To use the onbdtemplate utility to test a template:* on page 235. The U-Boot monitor prompt appears as shown in the following screen example.

```
[root@OnBoard root]# reboot
...
Hit any key to stop autoboot: 0
=> <INTERRUPT>
=>
```

2. Boot in single-user mode.

```
=> hw_boot single
```

3. When single user mode comes up, use the passwd command to change the root or admin user's password.

The following screen example shows changing the admin user's password.

```
[root@(none)/]# passwd admin
New password: admin_password
Re-enter new password: admin_password
Password changes
passwd; password updated successfully
[root@(none)/]#
```

4. Restart the OnBoard appliance to return to multiuser mode.

```
[root@OnBoard root]# reboot
```

The root or admin user should be able to log in with the new password.

5. Reconfigure authentication as desired.

## Web manager stops responding

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 /]# /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 -ef | grep apache
10131 nobody 3864 S /usr/local/apache2/bin/httpd -k start
```

If a line like the one in the previous screen example appears, the web application successfully restarted.

## Firmware image is corrupted

Information in *Boot file location* on page 272 gives an administrator who knows 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 only. 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. After you test the image and replace the Flash, if needed, you can then save the image to the removable Flash using the `create_cf` command.

You can use the `create_cf` command when troubleshooting problems with the boot image, as described under *To upgrade to a boot image from a network boot in U-boot monitor mode*: on page 277.

## Appendix B: Technical Specifications

Table B.1 lists the OnBoard appliance's specifications.

**Table B.1: Specifications**

| <b>Hardware</b>                         |                                                                                                                                                                                                                                                                                                    |
|-----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CPU                                     | Freescle Power QUICC III                                                                                                                                                                                                                                                                           |
| Memory                                  | 256 MB DDRAM/128 MB compact Flash                                                                                                                                                                                                                                                                  |
| Interfaces                              | 24/40 Ethernet 10/100 BT on RJ-45<br>1 RS-232 console on RJ-45<br>1 RS-232 DTE on RJ-45 for power manager or external modem<br>1 10/100/10000 BT Ethernet on RJ-45 for primary user connections<br>1 10/100 BT Ethernet on RJ-45 for user connections to a second network or failover from primary |
| Dual 32/16 bit PCMCIA Slots Supporting: | Supported PCMCIA card types                                                                                                                                                                                                                                                                        |
| Enclosure                               | Steel                                                                                                                                                                                                                                                                                              |
| Dimensions (WxDxH)                      | 17 in x 12 in x 1.75 in<br>43.18 cm x 80 cm x 4.45 cm                                                                                                                                                                                                                                              |
| <b>Environmental</b>                    |                                                                                                                                                                                                                                                                                                    |
| Operating Temperature                   | 50° F to 122° F<br>10° C to 50° C                                                                                                                                                                                                                                                                  |
| Storage Temperature                     | -40° F to 185° F<br>-40° C to 85° C                                                                                                                                                                                                                                                                |
| Humidity                                | 5% to 90% noncondensing                                                                                                                                                                                                                                                                            |
| <b>Electrical</b>                       |                                                                                                                                                                                                                                                                                                    |
| Power                                   | Universal AC, single or dual 100-240 VAC<br>50/60Hz<br>1.4 A max<br>Dual DC<br>36 to 75 VDC<br>5 A max input current                                                                                                                                                                               |

Table B.2 lists the OnBoard appliance's applicable standards and certifications.

**Table B.2: Standards and Certifications**

| Country/Region        | Standards and Certifications                                    | Scope                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-----------------------|-----------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Australia/New Zealand | C-Tick                                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Canada                | Industry Canada Equipment Standard for Digital Equipment (ICES) | ICES 003 Issue 4 (February 2004)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|                       | Canadian Standards Association (CSA)                            | CAN/CSA-C22.2 No. 60950-1-03-Information Technology-Safety-Part 1: General Requirements                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| European Union        | CE mark relevant directives                                     | EMC directive: <ul style="list-style-type: none"> <li>EN55022: 1998 + A1:2000, Class A Emission-Information Technology Equipment-Radio Disturbance Characteristics-Limits and methods of measurement (CISPR 22:2203, + A1:2004)</li> <li>EN55024: 1998 + A1:2001, Immunity Requirements-Information Technology Equipment - Immunity Characteristics - Limits and methods of measurement (CISPR 24:1997 + A2:2002)</li> </ul> Safety Directive: <ul style="list-style-type: none"> <li>EN60950-1:2001-Information-Technology Equipment-Safety-Part 1: General Requirements</li> </ul> |
| USA                   | Federal Communications Commission (FCC)                         | FCC Part 15 Class A                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

**CAUTION:** To comply with FCC and CE certification requirements, use shielded cables when connecting devices to the Ethernet ports.

## Appendix C: Safety Information

Follow the precautions in this appendix when installing Avocent products. Failure to observe the listed precautions may result in personal injury or damage to equipment. Failure to observe compliance requirements makes the equipment no longer compliant.

### General safety precautions

Observe the following general safety precautions when setting up and using Avocent equipment.

- Follow all cautions and instructions marked on the equipment.
- Follow all cautions and instructions in the installation documentation or on any cautionary cards shipped with the product.
- Do not push objects through the openings in the equipment. Dangerous voltages may be present. Objects with conductive properties can cause fire, electric shock, or damage to the equipment.
- Do not make mechanical or electrical modifications to the equipment.
- Do not block or cover openings on the equipment.
- Choose a location that avoids excessive heat, direct sunlight, dust, or chemical exposure, all of which can cause the product to fail. For example, do not place an Avocent product near a radiator or heat register, which can cause overheating.
- Connect products that have dual power supplies to two separate power sources, for example, one commercial circuit and one uninterruptible power supply (UPS). The power sources must be independent of each other and must be controlled by separate circuit breakers.
- For products that have AC power supplies, ensure that the voltage and frequency of the power source match the voltage and frequency on the label on the equipment.
- Products with AC power supplies have grounding-type three-wire power cords. Make sure the power cords are plugged into single-phase power systems that have a neutral ground.
- Do not use household extension power cords with Avocent equipment because household extension cords are not designed for use with computer systems and do not have overload protection.
- Make sure to connect DC power supplies to a grounded return.
- Ensure that air flow is sufficient to prevent extreme operating temperatures. Provide a minimum space of 6 inches (15 cm) in front and back for adequate airflow.
- Keep power and interface cables clear of foot traffic. Route cables inside walls, under the floor, through the ceiling or in protective channels or raceways.
- Route interface cables away from motors and other sources of magnetic or radio frequency interference.
- Stay within specified cable length limitations.
- Leave enough space in front and back of the equipment to allow access for servicing.



## **Rack or cabinet placement**

When installing Avocent equipment in a rack or cabinet, observe the following precautions:

- Ensure that the floor's surface is level.
- Load equipment starting at the bottom first and fill the rack or cabinet from the bottom to the top.
- Exercise caution to ensure that the rack or cabinet does not tip during installation and use an anti-tilt bar.

## **Table placement**

- Choose a desk or table sturdy enough to hold the equipment.
- Place the equipment so that at least 50% of the equipment is inside the table or desk's leg support area to avoid tipping of the table or desk.

## Appendix D: Device Configuration

### Tasks for configuring new devices

---

**NOTE:** The following device configuration requirements are unique to the OnBoard appliance:

---

- During device configuration, the OnBoard appliance administrator must assign a command template to each device.
- The administrator must also assign each device a private subnet, except in exceptional cases.
- The administrator may want 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).

### How the OnBoard appliance manages communications with devices

The OnBoard appliance 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 appliance 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.php> under the product name). 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 appliance administrators can test command templates and create new command templates if needed to deal with command differences.

An OnBoard appliance 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 appliance 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.

## Device type differences

**Table D.1: Device Type Differences**

| Protocol        | Device Type Differences                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>DRAC</b>     | 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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>IPMI 1.5</b> | Works without a command template and with the default scripts.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>IPMI 2.0</b> | <p>The OnBoard appliance administrator can support IPMI 2.0 type service processors with the IPMI 2.0 RCMP+ encrypted protocol in either of the two following ways:</p> <ul style="list-style-type: none"> <li>• Identify the SP as a IPMI 1.5 type which enables the OnBoard appliance to communicate with the 2.0-type service processor in v1.5 compatibility mode.</li> <li>• Copy the talk_generic_ipmi.exp onto talk_customN.exp and follow the directions within the file to modify the script for IPMI 2.0 support.</li> <li>• Modify the default ipmi script to support OEM extensions.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>RSA I</b>    | <p>The RSA I card uses a curses-based interface. The OnBoard appliance 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_customN.exp and following the directions within the script to modify the script for RSA I support. This script may not be compatible with all RSA I firmware versions, so it cannot be guaranteed to work.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>RSA II</b>   | <p>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 version 1.03/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:</p> <ul style="list-style-type: none"> <li>• 1.07/x235 was released before 1.03/x306.</li> <li>• 1.03/x360 is very different from 1.03/x205.</li> <li>• 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.</li> <li>• power on switches on the power for 1.03/x306 and 1.07/x235, but 1.03/x205 uses power -on.</li> <li>• 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.</li> </ul> <p>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.</p> <p>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.</p> |

## Additional uses for custom Expect scripts

Table D.2 lists some of the purposes for which an administrator might want to create a custom Expect script.

**Table D.2: 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 appliance, because Telnet is not encrypted. See <i>How Configuration Changes Are Handled</i> on page 55. In addition, see the notes in the following files in the <code>/libexec/onboard</code> directory: <ul style="list-style-type: none"> <li><code>bidi_login.exp</code></li> <li><code>ssh_login.exp</code></li> </ul> |
| Interact with the web interface of an SP.                                                                                                                                                                    | N/A                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| 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. | 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 appliance 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 appliance 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.
- 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 appliance.
- 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*: on page 233 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.
  - 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. 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.
3. 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.
4. 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.
5. 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.
6. If you cannot run one or more of the supported commands on the device, attempt to connect to the SP console.

---

**NOTE:** Even if the power management commands do not work on a new device, you can usually establish a connection to the SP's console.

---

7. If you cannot access the SP 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.

8. If you can access the server but still cannot access the SP's console, double-check the user name and password you are using against the user name and password that are configured for the device.
9. Once you have established the connection to the SP's console, type the help command, which gives you the syntax you need to use for the commands supported by the SP.
10. Note the syntax of the commands supported by the SP's console, and go to the next procedure.

**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 233, if the default templates do not work for a new device.

1. Log into the OnBoard appliance'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 and assigns 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 SP. 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 SP console whether or not they are authorized.

---

19. Save and quit the file.
20. Enter the `saveconf` command.
21. Log out from the console.
22. Log into the Web Manager as an administrative user and select the *Config-Devices* menu option.

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.

1. Log into the OnBoard appliance'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 appliance.
8. Go to *To use the `onbdtemplate` utility to create a new template:* on page 234.

## 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 SPs and devices. Table D.3 lists the default command templates and describes type types of devices to which they apply.

**Table D.3: Default Command Templates**

| Template                        | Type of Device                                 |
|---------------------------------|------------------------------------------------|
| <code>devconsole.default</code> | Devices that support access to their consoles. |
| <code>drac.default</code>       | DRAC III/XT type devices.                      |

**Table D.3: Default Command Templates (Continued)**

| Template            | Type of Device                                                                                                                                      |
|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| 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         | <ul style="list-style-type: none"> <li>• IPMI 1.5 type devices</li> <li>• Any type device when only native IP access is being configured</li> </ul> |

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
 authtype = local
 group = fremont
 databuf = default
 subnet = privnet1
 description = IBM xSeries E306 in Fremont
 template = rsa.default
```



```
[rack1_dev2_compaq_ilo]
 type = ilo
 ip = 10.0.0.2
 real_ip = 192.168.0.2
 virtual_ip = 10.0.0.2
 authtype = local
 group = fremont
 databuf = default
 subnet = privnet1
 description = Compaq Proliant iLO 1.82 server
 template = ilo.default

[rack1_dev3_dell_drac]
 type = drac
 ip = 10.0.0.3
 real_ip = 172.10.0.1
 virtual_ip = 10.0.0.3
 authtype = local
 group = fremont
 databuf = default
 subnet = privnet2
 description = Dell DRAC III/XT server
 template = drac.default
```

```
[au_rack1_dev4_newisys_ipmi]
 type = ipmi_1.5
 ip = 10.0.0.4
 real_ip = 172.10.0.2
 virtual_ip = 10.0.0.4
 authtype = local
 group = brisbane
 databuf = default
 subnet = privnet3
 description = Newisys IPMI 1.5 server
 template =

[au_rack1_dev5_cisco_router]
 type = devconsole
 ip = 10.0.0.5
 real_ip = 172.10.0.3
 virtual_ip = 10.0.0.5
 authtype = local
 group = brisbane
 databuf = default
 subnet = privnet3
 template = devconsole.default
 description = CISCO router
```

Note that the device with IPMI\_1.5 type does not have a template.

## Issues affecting configuration of RSA-type SPs

RSA I devices work differently from RSA II devices and recognize different commands. An 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 `customN` 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 233 describes steps the OnBoard appliance 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 an SP 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 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 *OnBoard Appliance Authentication Options* on page 24 and *OnBoard User and Group Configuration Options* on page 29.

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 123cycl to 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 appliance Expect scripts

The Expect scripts are located in the `/libexec/onboard` directory identified with the `.exp` suffix. Table D.4 lists each of the defined device types with the name of the associated Expect script.

**Table D.4: Default Device Types and Corresponding Expect Scripts**

| Device Type    | Expect Script                    |
|----------------|----------------------------------|
| iLO            | <code>talk_ilo.exp</code>        |
| RSA II         | <code>talk_rsa_II.exp</code>     |
| DRAC           | <code>talk_drac.exp</code>       |
| IPMI 1.5       | <code>talk_ipmi_1.5.exp</code>   |
| device console | <code>talk_devconsole.exp</code> |

Three additional custom types (`custom1`, `custom2` and `custom3`) allow OnBoard appliance administrators to create up to three customized scripts. Table D.5 shows the names of the Expect scripts associated with each of the custom types.

**Table D.5: Custom Device Types and Corresponding Expect Scripts**

| Device Type           | Expect Script                 |
|-----------------------|-------------------------------|
| <code>custom 1</code> | <code>talk_custom1.exp</code> |
| <code>custom 2</code> | <code>talk_custom2.exp</code> |
| <code>custom 3</code> | <code>talk_custom3.exp</code> |

By default, the `talk_customN.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 customN 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_customN.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.

Contact your Avocent representative if you need additional support for creating a custom Expect script.

## Example of creating a custom IPMI-type script

The OnBoard appliance uses `ipmitool` commands to communicate with IPMI 1.5 type service processors. The OnBoard appliance 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 appliance 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 an SP 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 `sponconsole`. When the second argument is `sponconsole`, any other number of arguments may follow; all arguments entered after the `sponconsole` action are collected into a single command to be executed in the device's native command interface.

```
talk_type.exp servername sponconsole [command1|command2]|... commandN]
```

### **servername**

The `servername` is the alias configured for the server or device on the OnBoard appliance, 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.

### **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 246 for the correct way to handle an unexpected action argument.

**sensors**

Asks the SP for a sensor reading and display service processor sensor output on standard output.

**poweron**

Asks the SP to power up its server.

**poweroff**

Asks the SP to power down its server.

**powercycle**

Asks the SP to reboot its server.

**powerstatus**

Asks the SP if its server is powered up.

**reset**

Asks the SP to reset its server.

**sel**

Asks the SP to retrieve the System Event Log and display the SEL contents on standard output.

**clearsel**

Asks the SP to clear the System Event Log.

**spconsole**

The native command line of the SP. Enters interactive pass-through mode. The script authenticates with the SP, then connects the SP output directly to its standard output and its standard input to the SP 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 enters a console session 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 exit codes shown in Table D.6.

**Table D.6: Expect Script Exit Codes**

| Exit Code | Definition                                                                                             |
|-----------|--------------------------------------------------------------------------------------------------------|
| 0         | Success                                                                                                |
| 1         | Unexpected output from service processor/device, or another error in an SP protocol (such as time-out) |
| 2         | Bad command line (such as an incorrect number of arguments)                                            |
| 3         | Action argument is not valid for the SP/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.

## Address configuration for connected devices

Table D.7 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 D.7: Tasks for Creating Addresses to Assign to Connected Devices**

| Task                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Where Described                                                                                                                                                                                                                                                                                                        |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Private IP addresses must be defined by the creation of at least one <i>private subnet</i>.<br/>A private subnet must be created for each IP address range used by the connected devices.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                     | <ul style="list-style-type: none"> <li>• <i>Why define private subnets?</i> on page 249</li> <li>• <i>Configuring a private subnet</i> on page 250</li> <li>• <i>Example 1: Private Subnet Configuration</i> on page 251</li> <li>• <i>Example 2: Two Private Subnets and VPN Configuration</i> on page 254</li> </ul> |
| <p>Private subnet(s) should use IP addresses from one of the three IP address ranges reserved for use on internal networks.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | <ul style="list-style-type: none"> <li>• <i>Using reserved IP addresses for private IP addressing</i> on page 248</li> </ul>                                                                                                                                                                                           |
| <p>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 appliance's DHCP server <code>dhcp.conf</code> configuration file.</p>                                                                                                                                                                                                                                                                                                                                                          | <ul style="list-style-type: none"> <li>• <i>Options for assigning IP addresses to connected devices</i> on page 271</li> </ul>                                                                                                                                                                                         |
| <p>A <i>virtual network</i> may be created in the following cases:</p> <ul style="list-style-type: none"> <li>• To hide a device's private IP addresses from non-administrative users who are not configured for native IP access.</li> <li>• When it is desired that multiple non-contiguous private subnets be supported by a single network route (or, in the case of IPSec, a single tunnel) on the client for VPN or native IP access. This would be the case when connected devices are already configured using IP addresses from multiple address ranges and it is not feasible to change previously-defined device IP addresses.</li> </ul> | <ul style="list-style-type: none"> <li>• <i>Why define virtual (DNAT) addresses?</i> on page 264</li> <li>• <i>To Configure IP Addresses From Multiple Ranges</i></li> <li>• <i>Example 3: Virtual network with two private subnets and VPN configuration</i> on page 264</li> </ul>                                   |

**Table D.7: Tasks for Creating Addresses to Assign to Connected Devices (Continued)**

| Task                                                                                                                                                                                                                                                                                                                         | Where Described                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Any user who needs native IP access to the OnBoard appliance needs to create a named VPN connection profile, then to create a VPN tunnel to the OnBoard appliance 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. | <ul style="list-style-type: none"> <li>• <i>Routing requirements for native IP access</i> on page 251</li> <li>• <i>IPSec VPN configuration for example 2</i> on page 258</li> <li>• <i>PPTP VPN configuration for example 2</i> on page 260</li> <li>• <i>Enabling native IP and accessing a device's native features using real IP addresses for example 2</i> on page 262</li> <li>• <i>IPSec VPN configuration for example 3</i> on page 267</li> <li>• <i>PPTP VPN configuration for example 3</i> on page 269</li> <li>• <i>Enabling native IP and accessing a device's native features using virtual network addresses for example 3</i> on page 270</li> </ul> |

## Using reserved IP addresses for private IP addressing

The OnBoard appliance 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 D.8 shows the reserved IP address ranges for internal networks.

**Table D.8: 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                        |

See <http://www.rhebus.com/techinfo/iprange.htm#ip1> for recommendations about which ranges to use for various sizes of organizations and for avoiding address conflicts.

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 Cyclades OnBoard appliance 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 appliance for the following purposes:

- To define a private OnBoard appliance address for the OnBoard appliance 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 appliance's native IP access facility.

The private Ethernet ports are accessed through the priv0 interface on the OnBoard appliance, which interacts with connected devices through an internal switch.

The OnBoard appliance attempts to reach a device that does not have a private subnet assigned by attempting to contact it through the OnBoard appliance's default route. Therefore, unless the OnBoard appliance 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 appliance. In almost all cases, devices are on the private side of the OnBoard appliance 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 264.)
- 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 appliance 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 appliance's private ports.
- Designating one of the IP addresses within the specified range to be used by the OnBoard appliance. The OnBoard-side address must be used by users when creating a IPsec VPN connection to enable native IP access.

The OnBoard appliance uses the specified information to create a route to the private subnet.

The range of IP addresses is derived from the information shown in Table D.9, which the administrator supplies to define a private subnet:

**Table D.9: 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 appliance. The OnBoard appliance 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 appliance uses the device's IP address when talking to a device, and devices use the OnBoard appliance's assigned address when talking the OnBoard appliance.

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 appliance 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 251
- *Example 2: Two Private Subnets and VPN Configuration* on page 254

## Routing requirements for native IP access

As documented in the Cyclades OnBoard Service Processor Manager User Guide, users who are authorized for native IP access need to create a IPSec or PPTP VPN connection before gaining native IP access.

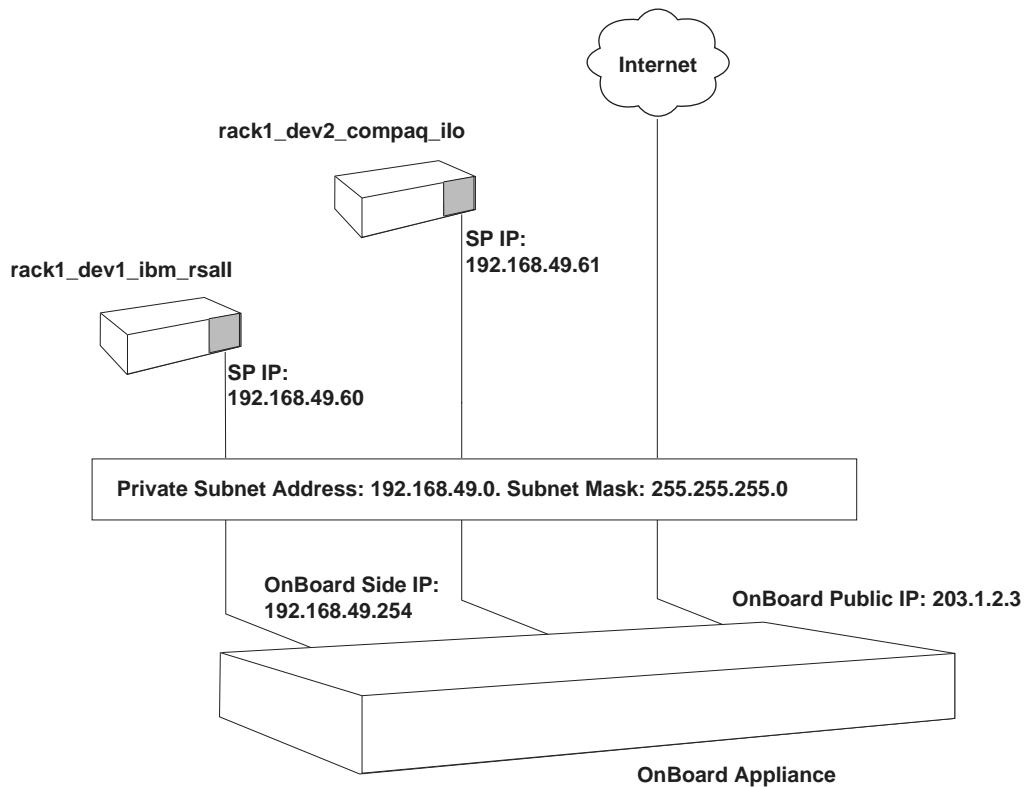
Any routes needed for IPSec VPN can be configured as part of the IPSec connection by setting the nexthop to the IP address of the desired network or host route and setting the boot action to Add and route.

Any route(s) needed for PPTP must be configured manually.

See *IPSec VPN configuration for example 2* on page 258, *PPTP VPN configuration for example 2* on page 260, *IPSec VPN configuration for example 3* on page 267 and *PPTP VPN configuration for example 3* on page 269, which discuss routing requirements for the two types of VPN connections and show example routes.

### Example 1: Private Subnet Configuration

Figure D.1 shows a private subnet configuration example.



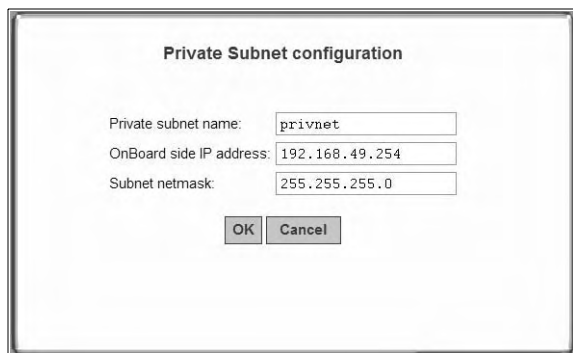
**Figure D.1: Example 1: Private Subnet**

In Figure D.1, two devices are connected to the OnBoard appliance. The public Ethernet port on the OnBoard appliance 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 appliance's private network: 192.168.49.60 and 192.168.49.61,
- A third private IP address within the same range to the OnBoard appliance: 192.168.49.254.

Figure D.2 shows the values the administrative user would enter in the Web Manager to configure the private subnet shown in Figure D.1.





**Private Subnet configuration**

Private subnet name:

OnBoard side IP address:

Subnet netmask:

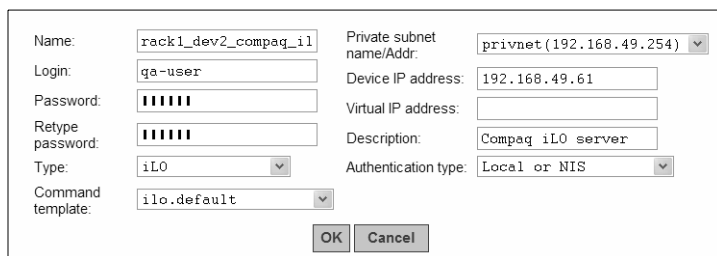
**Figure D.2: Private Subnet Configuration Example**

Figure D.2 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 D.2 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 D.1.



Name:  Private subnet name/Addr:

Login:  Device IP address:

Password:  Virtual IP address:

Retype password:  Description:

Type:  Authentication type:

Command template:

**Figure D.3: Example 1: Device Configuration Example**

As shown in the following example, the new private subnet name and the OnBoard appliance-side IP address and subnet mask from Figure D.2 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
```

### **Example 2: Two Private Subnets and VPN Configuration**

Figure D.4 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.

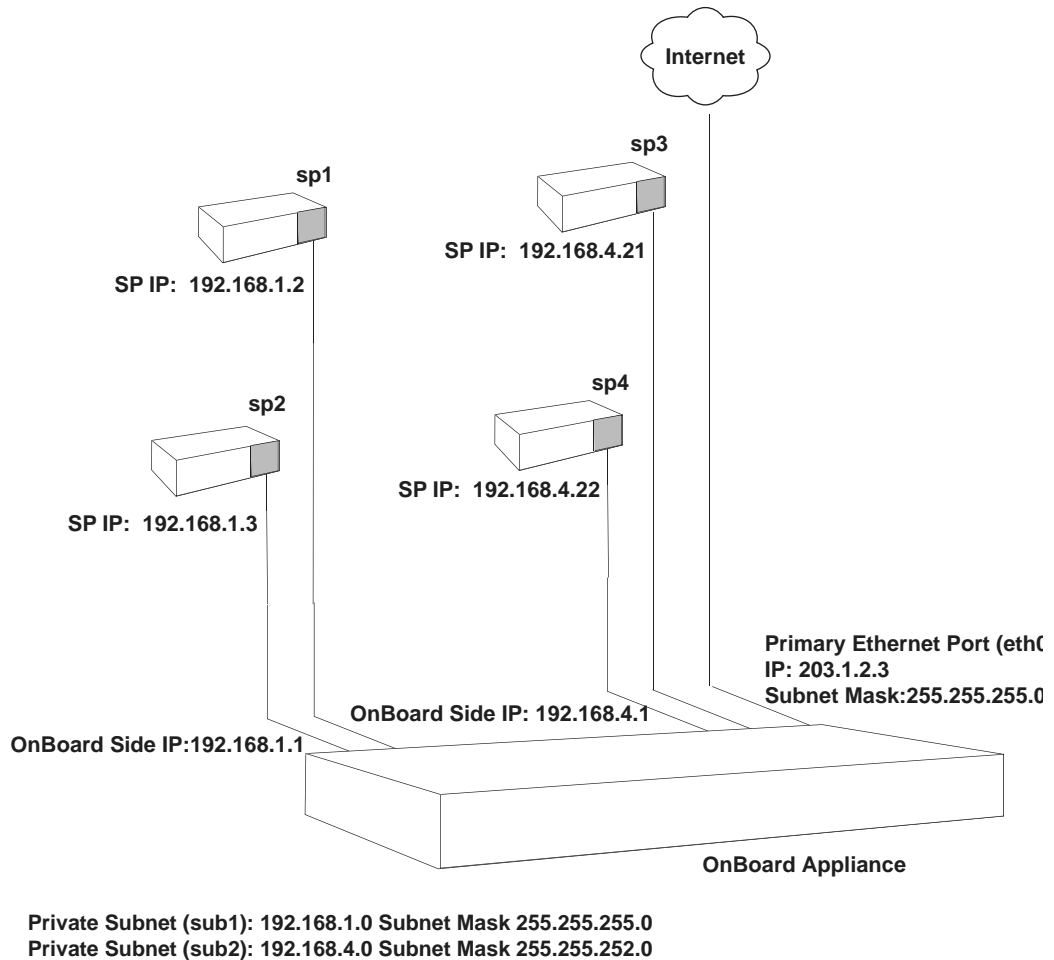


Figure D.4: Example 2: Two Private Subnets

## Two private subnets and user configuration for example 2

Configuration of the private subnets shown in Figure D.4 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 `pr iv0` by defining the OnBoard appliance side IP addresses and netmasks shown in Figure D.4 and listed here:

- Private subnet sub1
- OnBoard appliance side IP address: 192.168.1.1
- Subnet mask: 255.255.255.0

The above values define a range between 192.168.1.0 and 192.168.1.255 = 256 addresses, of which 254 are usable.

- Private subnet sub2
- OnBoard appliance side IP address: 192.168.4.1
- Subnet mask: 255.255.252.0

The above values define a range between 192.168.4.0 and 192.168.7.255 = 1024 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.

Figure D.5 shows the values entered on the Web Manager Network-Private subnet screen to implement the private subnets in this example.

| Subnet name | IP Addr     | Netmask       | Action |        |
|-------------|-------------|---------------|--------|--------|
| sub1        | 192.168.1.1 | 255.255.255.0 | Edit   | Delete |
| sub2        | 192.168.4.1 | 255.255.252.0 | Edit   | Delete |
| Add Subnet  |             |               |        |        |

**Figure D.5: Example 2: Values for Configuring Two Subnets**

As shown in the example output from the ifconfig command on the OnBoard appliance below, both private subnet names are assigned as aliases to the priv0 interface and the OnBoard appliance-side IP addresses and subnet masks from Figure D.5 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
```

The configuration of the devices shown in Figure D.4 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.

Figure D.6 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.

| Name | Subnet            | IP Address   | Type     | Description                    |      |        |
|------|-------------------|--------------|----------|--------------------------------|------|--------|
| sp1  | sub1(192.168.1.1) | 192.168.1.2  | RSA II   | IBM xSeries E306               | Edit | Delete |
| sp2  | sub1(192.168.1.1) | 192.168.1.3  | iLO      | Compaq Proliant iLO 1.7 server | Edit | Delete |
| sp3  | sub2(192.168.4.1) | 192.168.4.21 | DRAC     | DRAC III/XT server             | Edit | Delete |
| sp4  | sub2(192.168.4.1) | 192.168.4.22 | IPMI 1.5 | Newsys IPMI 1.5 server         | Edit | Delete |

Add new device

**Figure D.6: Example 2: Four Devices Configured on the Config -Devices Screen**

The OnBoard appliance 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.

Figure D.7 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.

Edit allSPs's device access privileges.

| Name | Sensors | Power | Event log | Service Processor Console | Device Console | Native IP |      |        |
|------|---------|-------|-----------|---------------------------|----------------|-----------|------|--------|
| sp1  | no      | no    | no        | no                        | no             | yes       | Edit | Delete |
| sp2  | no      | no    | no        | no                        | no             | yes       | Edit | Delete |
| sp3  | no      | no    | no        | no                        | no             | yes       | Edit | Delete |
| sp4  | no      | no    | no        | no                        | no             | yes       | Edit | Delete |

OK

**Figure D.7: Example 2: Configuring a User Account for Native IP Access to All Devices**

A VPN connection must exist before a user can access native IP management features on a device. Table D.8 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 D.8: Examples for Creating IPsec and PPTP VPN Connections for Example 2**

| Type of VPN                    | Where Documented                                         |
|--------------------------------|----------------------------------------------------------|
| Create an IPsec VPN connection | <i>IPsec VPN configuration for example 2</i> on page 258 |
| Create a PPTP VPN connection   | <i>PPTP VPN configuration for example 2</i> on page 260  |

## 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 255 is completed, a VPN connection must be created. This example shows the configuration steps that must be performed by the OnBoard appliance 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 appliance 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 appliance.
- 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 appliance's public IP addresses)
  - Left nexthop: leave blank if the user's workstation and the OnBoard appliance are able to exchange packets.

---

**NOTE:** The user can test whether the user's workstation can access the OnBoard appliance by entering the OnBoard appliance'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 appliance 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 appliance 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.

Figure D.9 shows the configuration on the 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.

The screenshot shows a dialog box titled "IPSec Add new connection" for a connection named "connSub1". The configuration is as follows:

- Connection name: connSub1
- Authentication protocol: ESP
- Authentication method: Shared secret
- Preshared key: dkdkkd
- Remote ("Right")**
  - ID: @workstation
  - IP address: 12.34.56.78
  - Next hop: (empty)
  - Subnet: (empty)
- Local ("Left")**
  - ID: @onboard
  - IP address: 203.1.2.3
  - Next hop: (empty)
  - Subnet: 192.168.1.0/24
- Boot action: Ignore

Buttons for "OK" and "Cancel" are at the bottom.

**Figure D.9: Example 2: Configuring IPSec Access to a Private Subnet and Two Devices**

In addition, the OnBoard appliance 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 appliance.

The OnBoard appliance 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 appliance administrator to create an IPSec VPN connection profile on the user's workstation.

If the OnBoard appliance administrator sends the relevant portions of the `ipsec.conf` file from the OnBoard appliance'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 262.

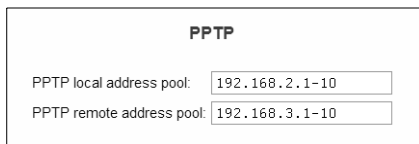
## PPTP VPN configuration for example 2

After the private subnets, device and user account configuration in *Two private subnets and user configuration for example 2* on page 255 is completed, a VPN connection must be created. This example shows the configuration steps that must be performed by the OnBoard appliance administrator and by a user on a remote workstation for setting up a PPTP VPN connection<sup>1</sup> that would enable the authorized user `allSps` to access `sp1`, `sp2`, `sp3` and `sp4`.

The OnBoard appliance administrator must do the following to enable the PPTP client:

- Make sure that the PPTP service is enabled.
- Configure PPTP on the OnBoard appliance.

Figure D.10 shows an example PPTP configuration on the Network-VPN connections screen.



The screenshot shows a configuration window titled "PPTP". It contains two input fields for address pools. The first field is labeled "PPTP local address pool:" and contains the value "192.168.2.1-10". The second field is labeled "PPTP remote address pool:" and contains the value "192.168.3.1-10".

**Figure D.10: PPTP VPN Configuration Example: Address Pools**

Figure D.10 shows the following address pools:

- PPTP local address pool: 192.168.2.1-10
- PPTP remote address pool: 192.168.3.1-10

---

**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 D.7.

---

1. A VPN tunnel must exist before a user can access native IP management features on a device.



- The user's account is configured for PPTP access to the OnBoard appliance as shown in Figure D.11.

Figure D.11 shows an example PPTP configuration on the Config-Users and groups screen.

The screenshot shows a configuration window for a user. At the top, there are text boxes for 'User Name' (containing 'sp1\_and\_sp2\_user') and 'Full Name' (containing 'User of SP1 and SP2'). Below these is a 'User Type' section with two radio buttons: 'Administrator' (unselected) and 'Normal User' (selected). A central message box reads: 'Changing the password field only changes the password managed by OnBoard.' Below this are several password-related fields: 'Password' and 'Retype password' (both masked with '|||'), a dropdown menu for 'PPP/PPTP access' set to 'PPTP (VPN) only', and another set of 'PPP/PPTP password' and 'Retype password' fields (both masked with '|||'). At the bottom are 'OK' and 'Cancel' buttons.

**Figure D.11: 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 appliance.  
The user can test whether the user's workstation can access the OnBoard appliance by entering the OnBoard appliance'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 appliance, configure the route.
- Use the PPTP client on the workstation to create the PPTP VPN connection profile, entering the following:
  - PPTP server address = OnBoard appliance public IP address (203.1.2.3)
  - Username = OnBoard appliance 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 appliance's end of the PPTP VPN tunnel.

When the PPTP tunnel is being activated, the OnBoard appliance 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 appliance 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 appliance would be 192.168.2.1.

- Enter the OnBoard appliance's PPTP-assigned address either in a browser or with ssh on the command line to access the OnBoard appliance. 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 be 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 be 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 262.*

### **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 258 or *PPTP VPN configuration for example 2* on page 260, the user uses the OnBoard side IP address configured for the appropriate private subnet to access the OnBoard appliance 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`.
  - Select 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 appliance's console and to access the rmenush 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-

- Enter **ssh** to execute the nativeipon command directly using the device alias

### 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 or a native management application.

A native web application may be accessed in one of the following ways:

- In the Web Manager on the OnBoard appliance, 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 appliance side address for the subnet where the device resides.

A native management application 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 SP:

- If the management application resides on the user's workstation, by bringing it up from there.
- If the management application resides on the SP, and is an executable that can be invoked on the command line, by accessing the SP's console first in one of the following two ways:
- Invoking ssh with the spconsole command.

-or-

In the Web Manager on the OnBoard appliance, clicking the Access Devices-*Service Processor Console* menu option.

-and

Bringing the management application up from the SP's command line.

- The console of the server on which the SP resides, in one of the following two ways:.
  - Invoking ssh with the devconsole command/

-or-

- In the Web Manager on the OnBoard appliance, clicking the Access Devices-*Device Console* menu option.

## Why define virtual (DNAT) addresses?

A virtual network based on DNAT may 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 by a single network route, 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.

Table D.12 describes the information that defines a virtual network.

**Table D.12: Information Defining a Virtual (DNAT) Network**

| Field          | Description                                                                                                                                                                                                                                                                                                                                                          |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Address</b> | IP address to assign to the OnBoard appliance 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 appliance. The administrator would then have all the other addresses to assign to devices, except for 10.0.0.0 and 10.0.0.255. |
| <b>Netmask</b> | 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 D.6 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

The following figure shows the same configuration as Figure D.4, but with the addition of virtual IP addresses.

Figure D.13 shows an example of virtual network configuration that enables virtual addresses to be assigned to connected devices and to the OnBoard appliance. The administrator plans to assign virtual IP addresses in the 172.20.0.1 range to hide the real private subnet IP addresses.

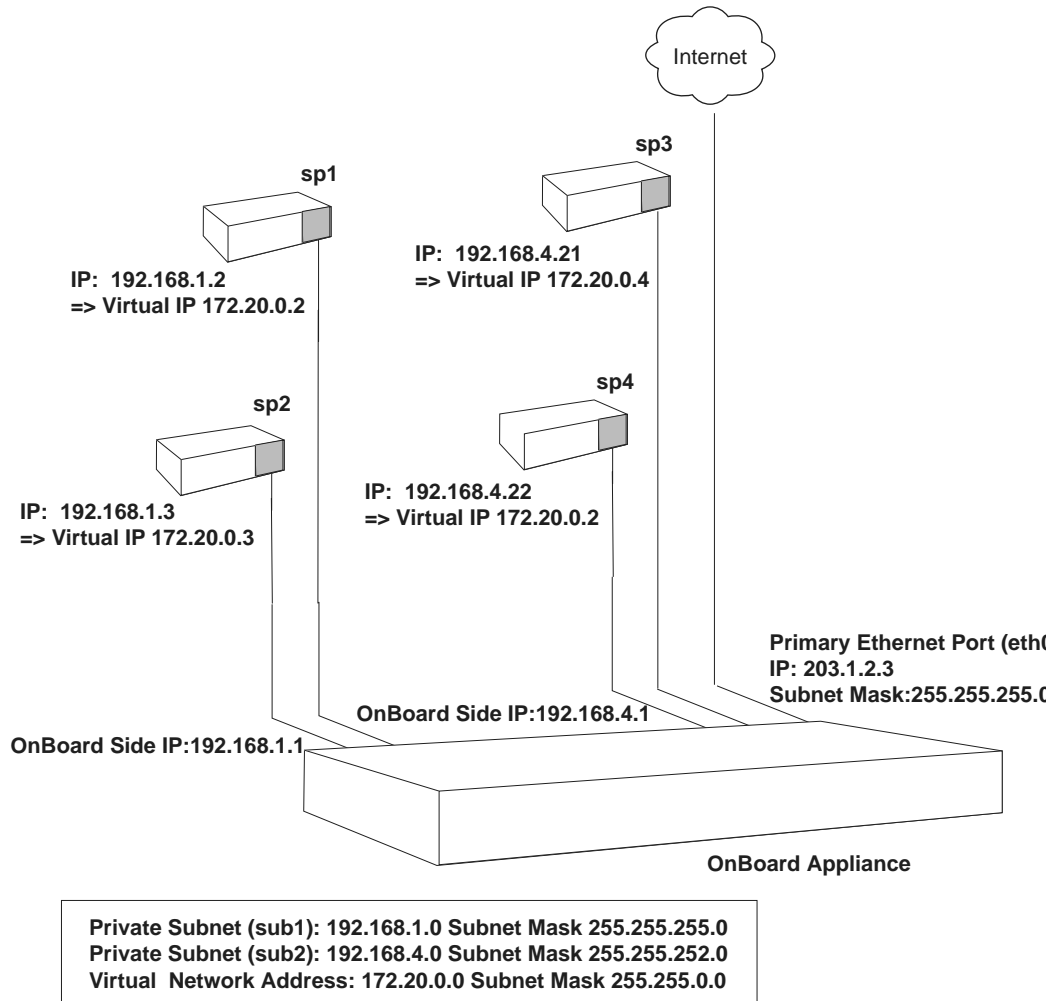


Figure D.13: Example 3: Virtual Network Configuration

**NOTE:** sp4 in Figure D.13 is an SP that does 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 appliance 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 D.13, the OnBoard appliance 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 appliance, in this case: 172.20.0.1
- Netmask: 255.255.0.0

Figure D.14 shows the desired values entered on the Web Manager Network-Private subnet: Add Subnet screen.

| Subnet name                                 | IP Addr     | Netmask                                  | Action |        |
|---------------------------------------------|-------------|------------------------------------------|--------|--------|
| sub1                                        | 192.168.1.1 | 255.255.255.0                            | Edit   | Delete |
| sub2                                        | 192.168.4.1 | 255.255.252.0                            | Edit   | Delete |
| <input type="button" value="Add Subnet"/>   |             |                                          |        |        |
| <b>Virtual Network (DNAT) configuration</b> |             |                                          |        |        |
| Address:                                    |             | <input type="text" value="172.20.0.1"/>  |        |        |
| Netmask:                                    |             | <input type="text" value="255.255.0.0"/> |        |        |

**Figure D.14: 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, Figure D.15 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 D.13.

|                   |                                          |                                                                         |                                                |
|-------------------|------------------------------------------|-------------------------------------------------------------------------|------------------------------------------------|
| Name:             | <input type="text" value="sp1"/>         | Private subnet name/Addr:                                               | <input type="text" value="sub1(192.168.1.1)"/> |
| Login:            | <input type="text" value="USERID"/>      | Device IP address:                                                      | <input type="text" value="192.168.1.2"/>       |
| Password:         | <input type="password" value="■■■■■■"/>  | Virtual IP address:                                                     | <input type="text" value="172.20.0.2"/>        |
| Retype password:  | <input type="password" value="■■■■■■"/>  | Description:                                                            | <input type="text" value="IBM xSeries E306"/>  |
| Type:             | <input type="text" value="RSA II"/>      | Authentication type:                                                    | <input type="text" value="Local or NIS"/>      |
| Command template: | <input type="text" value="rsa.default"/> |                                                                         |                                                |
|                   |                                          | <input type="button" value="OK"/> <input type="button" value="Cancel"/> |                                                |

**Figure D.15: Example 1: Device Configuration Example**

Figure D.16 shows the entries on the Devices screen for the devices shown in Figure D.13. 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)                                                                                                                                                                                                        |
|-------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Name:</b> sp1<br><b>IP:</b> 172.20.0.2<br><b>Description:</b> IBM xSeries E306               | <a href="#">Service Processor Console</a><br><a href="#">Device Console</a><br><a href="#">Power</a><br><a href="#">Reset</a><br><a href="#">Sensors</a><br><a href="#">Event Log</a><br>Native IP: Not available |
| <b>Name:</b> sp2<br><b>IP:</b> 172.20.0.3<br><b>Description:</b> Compaq Proliant iLO 1.7 server | <a href="#">Service Processor Console</a><br><a href="#">Device Console</a><br><a href="#">Power</a><br><a href="#">Reset</a><br><a href="#">Sensors</a><br><a href="#">Event Log</a><br>Native IP: Not available |
| <b>Name:</b> sp3<br><b>IP:</b> 172.20.0.3<br><b>Description:</b> DRAC III/XT server             | <a href="#">Service Processor Console</a><br><a href="#">Device Console</a><br><a href="#">Power</a><br><a href="#">Reset</a><br><a href="#">Sensors</a><br><a href="#">Event Log</a><br>Native IP: Not available |
| <b>Name:</b> sp4<br><b>IP:</b> 192.168.4.22<br><b>Description:</b> NewlSys IPMI 1.5 server      | <a href="#">Service Processor Console</a><br><a href="#">Device Console</a><br><a href="#">Power</a><br><a href="#">Reset</a><br><a href="#">Sensors</a><br><a href="#">Event Log</a><br>Native IP: Not available |

**Figure D.16: 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 266 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 258, 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 258, except the OnBoard appliance administrator must configure the Left subnet: by entering 172.20.4.0/22 to configure the connection to the virtual network.

Figure D.17 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 D.17: Example 3: IPSec Connection Configuration for Access to sub1 Private Subnet and sp1 and sp2 Devices**

As in the earlier example, the OnBoard appliance 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 appliance.

The OnBoard appliance 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 appliance administrator to create an IPSec VPN connection profile on the user's workstation.



If the OnBoard appliance administrator sends the relevant portions of the `ipsec.conf` file from the OnBoard appliance'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 262.

### **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 266 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 260, 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 appliance:

- Enter the `ifconfig` or `ipconfig` command on the command line of the user's workstation to discover the IP address assigned to the OnBoard appliance's end of the PPTP VPN tunnel.
- Enter the OnBoard appliance's PPTP-assigned address either in a browser or with `ssh` on the command line to access the OnBoard appliance. 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 260 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 262.

### 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 267 or *PPTP VPN configuration for example 3* on page 269, 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 262.

### 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 by entering the `http://172.20.0.1` URL.
  - Chose the *Access - 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:
  - Enter **ssh** to connect to the OnBoard appliance's console and to access the `rmenush` menu in one of the following ways:

```
ssh username:@172.20.0.1
```

```
ssh -t username:@172.20.0.1 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

- Enter **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 appliance, 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 appliance.

For example, see the following `ssh` command line entered by the user named `allSPs` to access `sp2` using the OnBoard appliance'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 SP:
  - If the management application resides on the user's workstation, by bringing it up from there.
  - If the management application resides on the SP, and is an executable that can be invoked on the command line, by accessing the SP'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 appliance, clicking the Service Processor Console link on the Access Devices screen.

-and-

Bringing the management application up from the SP's command line.

- The console of the server on which the SP 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 appliance, 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 *Address configuration for connected devices* on page 247, the OnBoard appliance administrator must do both of the following:

- Assign an IP address in the planned range of addresses when configuring each device on the OnBoard appliance, as described in *Parameters for configuring devices* on page 50.

- 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 appliance 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 appliance 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 an SP'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 appliance 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 68.

## Appendix E: Advanced Boot and Backup Configuration

This appendix provides information related to configuring boot file locations and managing configuration file changes on the OnBoard appliance.

This section has the following sections.

- *Boot file location* on page 272
- *Downloading a new software version* on page 274
- *Changing the boot image* on page 274
- *U-Boot network boot options and caveats* on page 276
- *Options for the create\_cf command* on page 278
- *Options for the restoreconf Command* on page 280

### Boot file location

How the OnBoard appliance boots is introduced at a high level in *Configuring the boot file location* on page 133 in the section on configuring boot in the Web Manager. 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 appliance uses a U-Boot boot loader that resides in soldered Flash memory and that automatically runs at boot time. U-Boot boots the OnBoard appliance from an image whose location is configurable. The image can reside either in a separate removable Flash memory on the OnBoard appliance or on a boot server on the network.

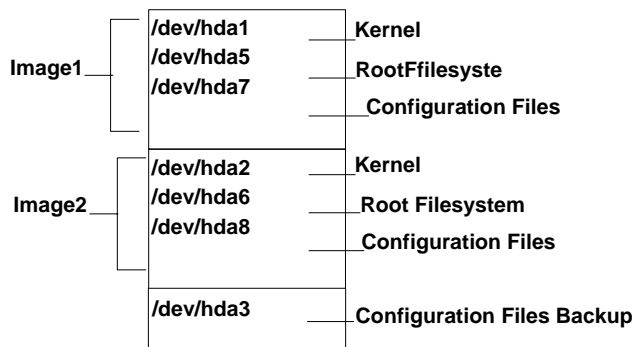
Up to two images may be stored at the same time on the OnBoard appliance's removable Flash. Each image on the removable Flash has three separate file systems mounted on three Linux partitions. The first partition for each image contains the kernel, the second partition contains the root filesystem mounted read only and the third partition contains the configuration files mounted read-write.

See <http://sourceforge.net/projects/u-boot>. for more about U-Boot in general.

The OnBoard appliance boots from alternate images as described below.

- The OnBoard appliance 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 appliance 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 appliance 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 the instructions about boot configuration. 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 E.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 RAM 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 appliance from the new location.

You have two other options if you cannot access the Web Manager:

- Use the `cycli` utility  
*See [To use the onbdtemplate utility to test a template](#): on page 235.*
- Boot in U-Boot monitor mode and use the available boot commands

See *To use the onbdtemplate utility to test a template:* on page 235.

### To boot from an alternate image using cycli:

1. Connect to the OnBoard appliance 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
```

3. Enter `get bootconf` 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.0830 IPaddress
```

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 appliance to U-Boot monitor mode.
- If boot fails, the OnBoard appliance 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:**

1. Access the OnBoard appliance command line through 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.
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. Go to U-Boot monitor mode.
2. Boot by entering hw\_boot followed by the single argument, as shown in the following example.

```
=> hw_boot single
```

The single-user # prompt appears, as shown in the following example.

```
[root@(none) /]#
```

**U-Boot network boot options and caveats**

When a network boot is performed with the U-boot net\_boot command, the OnBoard appliance boots from the specified image on the TFTP server. The image uses the RAM as the root file system. Network boots are useful for troubleshooting because the net-booted image can run even if there the OnBoard appliance's Flash memory is not usable.



Network boots are recommended only for troubleshooting and must not be used for normal operation of the OnBoard appliance. 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 278).

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 loaded.
- 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 Files* on page 81 and *Restoring Backed Up Configuration Files* on page 82).

### **To upgrade to a boot image from a network boot in U-boot monitor mode:**

Before performing this procedure, make sure that a copy of the latest boot image has been downloaded from the Cyclades ftp site (`ftp.cyclades.com/pub/cyclades/alterpath/onboard/released`) to a TFTP server that is accessible to the OnBoard appliance.

1. Log in as root and go to U-boot monitor mode.

If needed, see *To use the onbdtemplate utility to test a template:* on page 235.

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 appliance to use for network booting.

The format of the boot filename is: `zImage_onb_version_number.bin`. In the following example, the filename `zImage_onb_v120.bin` is used.

```
=> setenv ipaddr OnBoard appliance_IP_address
=> setenv serverip boot_server_IP_address
=> setenv bootfile boot_filename
```

See the following screen example.

```
=> setenv ipaddr 192.168.45.29
=> setenv serverip 192.168.45.127
=> setenv bootfile zImage_onb_v120.bin
```

3. Check that the environment variables are set properly with the printenv command.

```
=> printenv
ipaddr=192.168.45.29
serverip=192.168.45.127
bootfile=zImage_onb_v120.bin
```

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.

The following command example shows using the --factory\_default argument to restore the factory default configuration files at the same time.

```
[root@OnBoard root]# create_cf --doformat --factory_default
```

---

**CAUTION:** 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 278 for other options.

---

7. The following text appears when the operation completes.

```
Creation of image N completed.
...
```

8. Configure the OnBoard appliance to boot from Flash.

See *To use the onbdtemplate utility to test a template:* on page 235, if needed.

9. Enter the reboot command.

```
reboot
```

## Options for the create\_cf command

Administrators can use the create\_cf command when troubleshooting problems with the boot image, as described under *To upgrade to a boot image from a network boot in U-boot monitor mode:* on page 277. Use it carefully as described in this section.

---

**CAUTION:** 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.

---

**NOTE:** 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.

---

Table E.2 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 E.2: Options for the `create_cf` command**

| Option                         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>none</code>              | 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 <code>--doformat</code> and installs the image in <code>image1</code> . 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 |
| <code>-d device</code>         | Creates the image on the specified device. The default device is <code>/dev/hda</code> (the removable Flash memory). Make sure the filesystem is not mounted. Use the <code>-d device</code> option if you want to create the image in another location, such as on 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 <code>/dev/hdc</code> (PCMCIA slot 1) or <code>/dev/hde</code> (PCMCIA slot 2).)                          |
| <code>--factory_default</code> | Creates the image using factory default configuration files. By default, if this option is not entered, the configuration from the current partition is used, if valid. For more details, see <i>How Configuration Changes Are Handled</i> on page 55.                                                                                                                                                                                                                                                                                     |
| <code>--doformat</code>        | Rebuilds the partitions, erasing their contents. Creates the image as <code>image1</code> .                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <code>--dontformat</code>      | Does not format the compact Flash. The sizes of partitions <code>hda1-3</code> and <code>5-8</code> 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.                                                                                                                                                                                                                                                                            |
| <code>--imageN</code>          | Creates/replaces <code>imageN</code> , when <code>n=1   2</code> . Use this option to replace only the specified image without erasing both images. Changes the <code>currentimage</code> environment variable to boot from the image.                                                                                                                                                                                                                                                                                                     |

### Examples for `create_cf` command usage

Both examples assume you have done a network boot and you want to save the boot image from RAM.

#### To save a boot image to a compact Flash PCMCIA card:

1. Perform a network boot.
2. Insert a compact Flash PCMCIA card into a PCMCIA slot.

3. Enter the following command to save a copy of the image from RAM onto the card. The compact Flash card in the example is inserted into PCMCIA slot 1.

```
[root@OnBoard /]# create_cf -d /dev/hdc --image1
```

**To save a boot image into the Image2 area and restore the factory default configuration:**

1. Perform a network boot.
2. Unmount the resident removable Flash memory.
3. Enter the following command to save the image from RAM and restore the factory default configuration.

The example shows saving the image into the image2 area

```
[root@OnBoard /]# create_cf --factory_default --image2
```

## Options for the restoreconf Command

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>
```

## Appendix F: Technical Support

Our Technical Support staff is ready to assist you with any installation or operating issues you encounter with your Avocent product. If an issue should develop, follow the steps below for the fastest possible service.

**To resolve an issue:**

1. Check the pertinent section of this manual to see if the issue can be resolved by following the procedures outlined.

2. Check our web site at [www.avocent.com/support](http://www.avocent.com/support) to search the knowledge base or use the online service request.
3. Call the Avocent Technical Support location nearest you.



# INDEX

## Numerics

10/100 and 10/100/GE primary and secondary  
public Ethernet ports 2

1U device 1

## A

accessing

connected devices

controlling 23

the Web Manager 16

ACT 3

Active Directory schema, configuring 85

activity, capturing 24

adding rules for IP filtering chains 54

addressing scheme for devices 48

planning 103

administrative users

admin group, assigning on an authentication  
server 84

configuring interfaces 171

Wizard options 96

administrators 17, 93

ADSI Edit 85

AH authentication protocol 71

alarms

as a security feature 24

configuring 44, 45, 46

IPDU 6

triggers, configuring

email notifications 155

pager notifications 154

SNMP trap notifications 153

ALERT syslog severity level 40

alerts 24

anonymous logins to Cyclades' ftp server 191

Apache web server 66

authenticated users 39

authentication

as a security feature 23

configuring

for connected devices 11

for connected devices with cycli 208

for the OnBoard appliance with cycli 217,  
219

for the OnBoard appliance with Web  
Manager 151

supported methods

for the OnBoard appliance and connected  
devices 25

IPSec 71

authentication methods

introduction 24

AH 71

default

as defined in Moderate security profile 31

task for specifying 27

group authorizations configurable with 84

LDAP, RADIUS, TACACS+, configuring  
group authorizations with 84

OTP introduction 28

authentication servers

configuring

LDAP 147

list of tasks 27

- NIS 148
- RADIUS 149
- SMB 150
- TACACS+ 150
  - required for all authentication methods 24
- authorizations
  - as a security feature 23
  - bypassing in a custom security profile 30
- authorized users 39
  - accessing devices through OnBoard appliance 23
  - and Expect scripts 230
  - VPN configuration tasks 70, 73
- autodetect modem access type 43
- AUX ports
  - configuring for IPDU power management 44
  - illustrated 2
  - LEDs 4

## B

- backing up configuration files 81
- backup partition 274
- backups, configuring for files you add 82
- baud rate, modem 43
- /bin/do\_create\_cf\_ext2 script 60
- blade managers, connecting 11, 41
- bond0 41
- bonding 10
- boot
  - action, configuring for IPsec VPN 72
  - configuration fields and options 135
  - configuring at the U-Boot monitor 272
  - configuring in Web Manager 135, 136, 137
- boot image
  - checking if one exists 279

- locations 272
- partition locations 273
- problems, troubleshooting 278
- replacing 225, 272
- saving to compact Flash PCMCIA card 279
- troubleshooting problems with 225

- brackets, mounting 9
- broadcast IP address 15, 100, 174
- browser 16
- buttons
  - save and apply changes 81
  - unsaved changes 81

## C

### CA

*See certificate authority*

- cabinet mounting 9
- cables
  - connecting 9
  - DB-9 female to RJ-45 9
  - RJ-45 to DB-9 14
  - RJ-45 to RJ-45 Ethernet CAT5 10
- callback
  - configuration option 43
  - connection, used for troubleshooting 223
  - using to access the Web Manager 93
- card slots 5
- Cautions
  - changing admin passwords 97
  - closing PPTP VPN connections to prevent unauthorized access. 74
  - complying with FCC and CE certification requirements 11
  - create\_cf --doformat option 278
  - device IP address visibility 264



- disabling native IP before ending PPTP VPN connection 74
- Kerberos time/date synchronization requirements 145
- network boot image 279
- OTP 62
- private subnet requirements for devices 107, 139
- restricting OnBoard users' access 39
- risks from not changing administrator's passwords 97
- safety precautions 8
- shielded cable requirements for compliance with FCC and CE requirements, 227
- using snmpd without a VPN tunnel 35
- when adding users in the Wizard 108
- when changing or deleting private subnets 103
- when changing the default rmenu.sh menu 78, 79
- when creating a command template 235
- when creating filtering rules 53
- certificate signing request, generating 66
- chains, packet filtering 53
- circuit breakers 11
- command line
  - accessing through the console port 6
  - using ssh command on to access the OnBoard appliance 73
  - using to check for the PPTP address 74, 261, 269
- command templates
  - assigning to devices
    - overview 230
    - when not to assign 232
  - creating 230
  - table showing devices to which they apply 235
  - tasks for configuring a new device 230
  - testing 230
    - when not to use 238
- commands
  - commit 81
  - create\_cf utility 225, 278, 279
  - courses 231
  - cycli utility 27, 29, 53, 81
    - enabling data buffering 52
  - daemon.sh 224
  - ifconfig 261
  - ipconfig 74, 269
  - ipmitool 232
  - onbdtemplate utility
    - introduction 230
    - testing a template 235
    - using 239
    - using to create a new template 234
    - when to use 233
  - openssl 66
  - opiekey 63, 64
  - opiepasswd 63, 64
  - ping command 233
  - ps command 224
  - restoreconf command 82
  - saveconf 81
  - saveconf command 235
  - ssh command 73, 233
  - telnet command 233
  - using for troubleshooting 279
- communications
  - blocked between private Ethernet ports 41
  - proxied 23
- compact Flash PCMCIA card
  - saving the boot image on 279
  - using to mount the /mnt/opie directory for OTP support 60

- computer, connecting to the console port 6
- configsource environment variable 277
- configuration 13
  - boot 135
  - files 81
    - backed up 81, 274
    - factory default 55, 280
    - restoring 56
    - restoring to factory defaults 82
    - saving changes 56, 81
  - source of data during a network boot 277
- configuration\_files.gz backup file 81
- connecting cables 9
- console
  - accessing through dedicated Ethernet ports 47
  - accessing to restore factory defaults 82
  - destination for syslog messages 40
  - logout 235
- console access 11, 17
- console port 2, 6, 13, 14, 15, 17
  - LEDs 4
- create\_cf command 278
  - options 279
  - using to replace a corrupted image 277
  - using when troubleshooting 225
- CRIT syslog severity level 40
- crond daemon 45
- currentimage environment variable 274, 279
- curses commands 231
- custom security profile
  - with a default authorization method set 27
  - with the override authorizations feature set 30
- customizing
  - command templates 230
  - expect scripts 230
- Cyclades PM IPDUS
  - downloading software for 112
- Cyclades PM IPDUs 44
- Cyclades, downloading updates from 112, 192
  - ftp server for 191
- cycli utility
  - add command 204, 210
  - adding a user 63
  - adding/editing iptables rules 55
  - commands 204
  - commit command 211
  - configuring
    - alarms 44, 45, 46
    - authentication 27, 53
    - basic network parameters 14, 15
    - modems 42, 43
    - rules for IP filtering 53
    - services 32
    - users 29
  - delete command 211
  - detecting services starting and stopping 32
  - enabling data buffering 52
  - example scripts 52
  - exit command 211, 214
  - list command 213
  - quit command 214
  - quit! command 214
  - rename command 214
  - revert command 214
  - saving (committing) changes 53, 81
  - set command 215
  - shell command 215
  - show command 211
  - using to enable Web Manager access 13
  - version command 216

**D**

daemon.sh command, WEB option 224

daemons 45

daisy-chaining Cyclades PM IPDUs 21

data buffering

- introduction 24, 52

- as a security feature 24

- configuring for a device with cycli 220

- configuring the default with cycli 219

- configuring with Web Manager 138

- options for devices 50

data filtering, events generating syslog messages 39

date and time, configuring 132

DB-9 female to RJ-45 cable 9

DB-9 male COM port 14

DC models 2, 12

DEBUG syslog severity level 40

dedicated Ethernet ports 47

default route 44, 100, 172

- specifying 174

- when private subnets are not configured 103

defaults

- configuration files 280

  - restoring 82

- data buffering, configuring 52

- IP addresses

  - using to access the Web Manager 16

- OnBoard IP address, using to access 14

- packet filtering chains 53

- static IP address 172

Destination Network Address Translation

- See DNAT*

destinations for syslog messages 40

detected devices 186

/dev/hdc PCMCIA slot 1 device name 279

/dev/hde PCMCIA slot 2 device name 279

devconsole.default command template 235

device groups, assigning to devices 50

device management 23

- actions

  - event log 231

  - power 231

  - service processor console 231

device types 230

devices 11, 16, 23

- accessing native IP features on 73

- assigning an authentication method to

  - with vi 62

  - with Web Manager or cycli 27

- assigning private subnets to 51

- configuring 3, 17

- connecting 47

- console access through dedicated Ethernet ports 47

- controlling access to 23

- default authentication method 31

- detected 186

- supporting untested 51

DHCP 13

- configuring

  - for a failover device 100, 172, 173

  - in Web Manager 173

  - in Wizard 101

- default route, automatically assigned by DHCP server 44, 100, 172

- service requiring additional configuration 32

- when the server cannot be reached 172

DHCP server 13, 16

dial-ins 93

- introduction 42
- configuring OTP authentication for 61
- DNAT 103, 105
- DNS
  - configuring in Web Manager 174
  - name 13
  - server 171
- do\_create\_cf\_ext2 script 60
- domain name 171, 174
- domain name. 15
- downloading
  - firmware (software)
    - Cyclades PM IPDU 112, 192
    - OnBoard appliance 112, 192
  - release notes 233
- DRAC device type
  - command template 235
  - DRAC II devices 231
  - DRAC III/XT devices 231
  - DRAC IV devices 231
- drac.default command template 235
- dual-AC power supply 1
- dynamic IP address 16

**E**

- edit rule for packet filtering chain 54
- email address, configuring for system email 135
- email notifications, configuration options 45
- EMERG syslog severity level 40
- environment variables, currentimage 279
- ERROR syslog severity level 40
- escape sequence, device console 235
- ESP authentication protocol 71
- /etc/config\_files file
  - adding a new file to be backed up/restored 82

- certificate files pre-added to 67
- /etc/httpd/conf/ssl.key/server.key file 67
- /etc/mgetty.login.config file 61
- /etc/onboard\_templates.ini file 235
- /etc/pam.d/login file 61
- /etc/pam.d/otp file 61
- /etc/pam.d/otplocal file 61
- /etc/pam.d/sshd file 61
- /etc/raddb/server file 88
- eth0 and eth1 41
- Ethernet
  - cable 10, 11
  - failover 10
    - configuring 172
  - PCMCIA cards
    - connecting 10
    - eth2 and eth3 interfaces 41
    - using and configuring 10
- Ethernet ports
  - introduction 41
  - configuring a static IP address for 173
  - configuring, Web Manager 171, 173
  - private 2, 3, 11
  - public 4, 10
- event log management 231
- examples
  - configuration using the cycli utility 52
  - private subnet configuration 251
  - two private subnets and VPN 254
  - virtual network configuration with one private subnet 265
- Expect scripts
  - arguments 244
  - exit codes 246
  - talk\_customN.exp 231

- talk\_generic\_ipmi.exp 231
- talk\_rsa\_I.exp 231, 238
- using 230
- when a customized one is needed 233

external modems 42

- connecting 5

## F

factory default configuration files

- how stored and restored 55
- how to restore 55
- restoring
  - with the command line 82
  - with the create\_cf command 279
  - with the create\_cf command, example 280
  - with the restoreconf command 82

failover 10

- introduction 41
- configuration, Wizard 100, 102
- configuring 172, 173

files

- /etc/onboard\_templates.ini file 235
- /etc/raddb/server 88
- configuration, restoring 56
- configuration\_files.gz 81
- hdc.conf 145

firewall

- configuration introduction 53–55
- rules, configuring, Web Manager 174

firmware

- Cyclades PM IPDU, downloading from
  - Cyclades 112
- heading on the Cyclades downloads page 233
- image 279
- OnBoard appliance

- downloading from Cyclades 112, 192
- service processor, tested 232
- supported untested 51

## Flash memory

- OnBoard removable
  - partitions 279
  - upgrading firmware on 194
- PCMCIA card 279
  - saving the boot image on 279
- unusable, recovering from 276

flow control 43

format storage media, while creating a boot image 279

FORWARD packet filtering chain 53

## FTP

- site for downloading OnBoard appliance firmware 191

FTPD 32

## G

### gateway

- configuring in Web Manager 174
- configuring in Wizard 100

gateway IP address 15

grounded wire 12

### groups

- authorizations, configuring on authentication servers 84
- configuring with cycli 219
- configuring with Web Manager 140

## H

hdc.conf file, on the Kerberos KDC 145

hex screw 12

high-availability 41

host route 44

host settings Web Manager option 171

hostname 15

HTTP 31, 32, 93, 98

HTTPS 31, 32, 34, 93, 98

## I

IBM service processors 231

ICMP 31, 32

ifconfig command 41, 74, 261, 269

iLO devices, default command template for 236

ilo.default command template 236

image

file 192

software 279

INETD 32

info attribute, configuring on a Active Directory server 85

Info menu 186

INFO syslog severity level 40

information

about detected devices 186

about session status 186

about the system 186, 188

INPUT packet filtering chain 53

installation

advanced 19–21

basic 7–17

basic tasks 8

interfaces

configuring in Web Manager 171

*See also network interfaces*

Internet

access 10

intrusion, reducing risks of 97

inverted options for packet filtering 54

IP addresses 13

broadcast 174

default 16

DHCP, to access the Web Manager, using 16

dynamically assigned 16

gateway 15

of remote IPSec gateway 72

OnBoard appliance 106

planning 103

static 15

IP filtering, introduction 53–55

IPDUs

overcurrent status generating syslog messages 40

power management 44

IPMI 1.5

Expect script 231

IPMI 1.5 devices

command template requirements 236

compared to other device types 231

IPMI 2.0 devices 231

ipmitool command 232

IPSec

authentication methods 25

in the Moderate security profile 31

service requiring additional configuration 32

VPN

configuration tasks 72

connections 71

iptables introduction 53–55

## K

Kerberos authentication method 25, 71

KDC 145

Key Distribution Center (KDC) 145

keys generated for RSA public keys 71

## L

LAN 10

connecting the primary Ethernet port to 10

LDAP authentication method 25, 71

configuring for OpenLDAP server 84

configuring for Windows Active Directory 84

configuring group authorizations with 84

LDAP authentication servers

configuring in Web Manager 146

LEDs

for the AUX port 4

on private Ethernet ports 3

on public Ethernet ports 4

lightweight directory access protocol

*See LDAP*

Linux operating system

command line, viewing create\_cf options on 279

configuring PPTP on 73

support for IPsec and PPTP on 71

LK/SP 3

local

administrators, troubleshooting 223

authentication 25

fallback options 24

local area network 10

*See LAN*

logging, system 24

login shell 44, 78

rmenush 44, 78

logins

anonymous to ftp.cyclades.com 191

authentication options for 24

modem access type 43

tasks for configuring authentication for 27

## M

MAC address 41

Macintosh 73

MacOS X support for IPsec and PPTP 71

maintenance tasks not done using Web Manager 57

management access 11

management network

connecting to 41

management of connected devices 23

message filtering 40

levels, syslog 40

message logging 39–40

MindTerm applet

when a user connects to a console 59

using to create an SSH tunnel 59

/mnt/hda3/backup directory 81

/mnt/hda3/backup/configuration\_files\_gz file 81

/mnt/opie directory 60

modems

access type menu options 43

external 42

initialization string 43

introduction 42–43

tasks for configuring 42

types 5

used for troubleshooting 223

mounting

brackets 9

OnBoard appliance 9

MS-CHAPv2 71

MTU 100, 174

**N**

- native IP
  - command template for any device type 236
  - configuring access
    - through PPTP VPN tunnel 73
  - enabling
    - after creating PPTP VPN tunnel 74
    - after VPN tunnel is created 73
  - starting the VPN connection from a remote computer 70
- net\_boot command 274
- netmask 15, 106, 174
  - for IPSec VPN connections 72
- network
  - address 106
  - boot 276
  - configuration, checking for trouble 233
  - services 24
- network interfaces
  - configuring 171
    - a default route 44, 100, 172
    - Web Manager 171
    - Wizard 99
- network route 44
- network services 32
- NIS authentication server
  - configuring 147, 148, 149, 150, 153, 154, 155, 156
- Notes
  - /usr/sbin/ directory mounting 57
  - accessing an SP's console to find command syntax 233
  - adding groups to a Frame-Filter-Id definition 87
  - adding users 64
  - arbitrary assignment of PPTP IP address pools 260
  - condition for assigning a custom template to a device 243
  - configuration is per device not per port 187
  - configuring
    - a user as an administrative user on an LDAP server 85
    - authentication 11
    - groups on a RADIUS server 89
  - configuring groups on a TACACS+ authentication server 90, 91
  - configuring services 32
  - configuring support for untested devices and firmware 51
  - configuring the secondary Ethernet port 102
  - configuring users for PPP/PPTP 261
  - configuring users on an LDAP server for group access 86
  - connecting to an SP's console 233
  - cycli utility not displaying OTP authentication 62
  - daisy-chained IPDUs running the same firmware 21
  - daisy-chaining IPDUs 111
  - devices unreachable without private subnet 183
  - DHCP configuration of IP addresses 34
  - effects of selecting a default authentication type 31
  - handling unsupported sensors in command templates 234
  - HTTP disabled in secured profile 98, 169
  - invoking ssh with the -t option 245, 246
  - IP address used for the appliance's default route 174
  - IPDU master and slave units 119
  - Kerberos requirements for time and date synchronization 145



- login session time-outs 93
  - losing configuration file changes 211, 213
  - modem configuration with cycli 42
  - not all cycli parameters and values described 198
  - not using cycli user to configure new users 210
  - OTP authentication support 127
  - OTP secret pass phrase 64
  - PCMCIA cards occupying two card slots 19
  - powering the OnBoard appliance 21
  - powering with separate power sources 11
  - saving server.key and server.crt files 67
  - saving the image from RAM 279
  - setting a gateway IP address and a default route 79
  - slapd.conf file location on LDAP server 86
  - SNMP and the security profile 161
  - storing buffered data in separate files 59
  - testing access to the OnBoard appliance 258
  - unique device configuration requirements 230
  - users and groups on TACACS+ servers 90
  - using a crossover cable for terminal connections 14
  - using talk\_customN.exp scripts 246
  - using the default IP address 16
  - virtual network addresses unsupported 264, 265
  - virtual network advantages 73
  - VPN tunnel requirement for native IP access 260
  - Web Manager support for OTP authentication. 61
  - workaround for packets blocked by a firewall 259
- NOTICE syslog severity level 40
- notifications 24
- configuring 46
  - in security features table 24
- notifications of over-current states 6
- NTP service 32
- ## O
- off-the-shelf cables 10
- onbdtemplate utility
- introduction 230
  - details 239
  - procedure for using 234
  - use by the administrator 233
  - using to test a template 235
- OnBoard appliance
- 1040 DAC model 1
  - features overview 23
  - administrator 230
  - configuring a default route 44, 100, 172
  - granting access to VPN connections 70
  - how device communications are managed 230
  - IP address for the public interface 74
  - mounting brackets 9
  - requirements for device configuration 230
  - SNMP on 39
  - supported devices and firmware levels 230
  - system events generating syslog messages 39
  - to rackmount 9
  - understanding authentication on 24
  - unique security features 23
  - web server 66
- one time passwords in everything
- See OPIE*
- OpenLDAP authentication server 84
- openssl utility 66
- OpenSWAN 71
- opiekey command
- generating passwords for users 63, 64

- opiepasswd command
  - registering users 63, 64
- OTP authentication method
  - introduction for administrators 28
  - for dialing into PCMCIA modem or phone cards 43
  - generating passwords for users 63
  - OTP/Local 61
    - where supported 26
  - registering users 63
  - specifying the databases' location 60
  - tasks for configuring 28
  - where supported 26
- outlets, configuring 6
- OUTPUT packet filtering chain 53
- overcurrent alerts 40
- P**
- packet filtering
  - introduction 53–55
  - on the OnBoard appliance 53
  - overview 53
  - rules 53
- pager notifications 45
- partitions
  - checking partition size with create\_cf 279
  - rebuilding 279
  - reformatting with create\_cf 279
- passwd command 15
- password
  - administrative user 13
  - changing root's 16
  - root user, changing 17
- passwords 93
- PCMCIA cards
  - and create\_cf 279
- compact Flash
  - configuring 131
  - saving the boot image on 279
- Ethernet
  - configuring 129, 130
  - connecting 10
- Flash memory, saving the boot image on 279
- modem
  - beginning to configure 124
  - configuring 124
  - overview 42
  - modem, connecting 5
- PCMCIA slots 1, 5
- Phillips screwdriver 9, 10
- ping command 233
- planning
  - device IP addresses 103
- ports
  - console 6
  - RS-232 6
- positive wire to DC power 12
- power cords 11
- power management
  - commands 230, 233, 238
  - daisy-chaining Cyclades PM IPDUs 5, 21
  - device 231
  - on IBM servers using RSA II cards 231
- power on 230
- power sources 12
- power supplies 11
- power switches 11, 12
- PPP
  - authentication 25
  - modem access type 43

- user configuration settings 29
- using to access the Web Manager 93

PPTP 25, 29, 31, 32, 70, 71

- client 71, 74, 261
- password 74
- VPN
  - connections 73

pptp-linux 71

preshared key (PSK) 71

primary Ethernet port 10, 47

- configuring, Web Manager 171

priv0 41, 249

private Ethernet ports 2, 11, 47

private network 23, 41

private subnets

- caution when changing or deleting 103
- configuration example 251, 254
- configuring, Wizard 103
- device configuration task 230
- parameters for configuring 104

procedures

- basic installation 8

protocols, vulnerabilities not exposed on public network 23

proxied communications 23

ps command 224

PSK (preshared key) 71

public Ethernet ports 4, 10

public key

- SSL 66
- SSL certificate request 67

public network 23, 41

## Q

Quick Start Guide 9

## R

rackmounting 9

RADIUS authentication method 26

- configuring group authorizations with 84
- for PPTP VPNs 71

RADIUS authentication servers

- configuring
  - in Web Manager 148

RAM

- root filesystem in after network boot 274
- saving an image to Flash 194
- used to store a network boot image 274, 276
- used to store changes until they are saved 55

redundancy 10, 11

regular users 17

release notes 230, 233

remote administrators 24

- troubleshooting 223

removable Flash 274

restart

- persistence of configuration file changes after 55

restoration

- configuring for added files 82
- tasks for configuration files 82

restoreconf command

- factory\_default option 82
- options 280

restoring

- backed up configuration files 55
- configuration files 56
- factory default configuration files 55, 82

RJ-45 to DB-9 6 ft. CAT5 cable 14

RJ-45 to RJ-45 Ethernet CAT5 cable 9, 10

rmenush login shell, configuring 44, 78

- root user 16, 79
  - changing the password 17
- routers 10, 11
- routing
  - for the OnBoard appliance, understanding 44
  - specifying the OnBoard appliance's default route 44, 100, 172
- RPC 33
- RS-232 port 6
- RSA I devices 231
  - issues when configuring 238
- RSA II devices
  - default command template for 236
  - differences between devices of the same type 230
  - issues affecting configuration of 238
  - table of differences 231
- RSA public keys 71
- rsa.default command template 233, 236, 238
- rsa.limited.default command template 233, 236, 238
- RTN screw 12
- rules
  - configuring for packet filtering 53
  - hidden, for packet filtering 53
  - packet filtering 53
- S**
- safety precautions 9
- save and apply changes
  - button 81
  - using the cycli utility 81
- Save button on the Mgmt-Backup/restore screen 81
- saveconf command
  - backing up configuration changes 81
  - run as prerequisite to restoring backed up configuration files 82
  - saving a newly-configured template 235
- saving configuration file changes
  - procedures 81
  - tasks 56
- screwdriver 9
- screws 9, 10
- scripts
  - configuring backups for 82
  - Expect
    - how used for device communications 230
    - additional uses for 232
    - arguments 244
    - exit codes 246
    - location and customization options 242
  - talk\_customN Expect 243
  - using with IPMI 1.5 type devices 231
- secondary Ethernet port 10, 41
  - configuring, Web Manager 171
- security
  - changing admin user password 97
  - isolating devices from the public network 41
- security features unique to the OnBoard appliance 23
- security profiles 24
  - configuring on a new OnBoard appliance 17
  - custom 27
  - effect on authorizations 30
  - selecting or customizing, Wizard 98, 169
- self-signed certificates 34
- sensors
  - alarms 40
    - configuring 44, 45, 46, 156
  - events generating syslog messages 40
  - management on IBM servers with RSA II cards 231

- servers 11
  - authentication, configuring
    - LDAP 147
    - NIS 148
    - RADIUS 149
    - SMB 150
    - TACACS+ 150
  - syslog 40
- service processors 11
  - connecting multiple to a single private Ethernet port 41
  - connecting to OnBoard appliance
    - illustrated 47
    - multiple to a single private Ethernet port 41
  - console 233
    - access usually available 233
    - management actions on RSA 1 cards 231
  - hiding vulnerable protocols used by 23
  - IBM console management action 231
  - management features 23
- services
  - administration options described 32
  - controlled by security profiles 24, 30
- session status 186
- shared secret 71
- shipping box contents 9
- SMB authentication method 26
- SMB authentication server, configuring, in Web Manager 149, 150
- SMTP server, configuring for system email 135
- SNMP
  - configuration tasks 39
  - security profile configuration 31
  - service 32
  - trap notifications 45
  - v1, v2, v3 35
- software
  - downloading from Cyclades
    - Cyclades PM IPDUs 112
    - OnBoard appliance 191, 192
  - heading on the Cyclades downloads page 233
  - image
    - file pathname on ftp server 192
    - saving from RAM to Flash using create\_cf 279
  - upgrading
    - retaining configuration file changes 55
- SPs
  - See service processors*
- SSH
  - configuring OTP authentication for 61
  - enabled in moderate security profile 31
  - encryption 23
  - in MindTerm 59
  - service not requiring additional configuration 33
  - tunnel, administrative user creating using MindTerm 59
- ssh command 73, 74, 233, 262, 269
- SSL certificate requirements 34
- static IP address 15, 71, 173
  - configuring for Ethernet ports
    - Web Manager 173
    - Wizard 101
- subnets
  - configuring in Wizard 103
  - for IPsec VPN connections 72
  - supporting multiple 105
- switch 10, 11
- syslog
  - introduction 39–40

- message filtering levels 40
- message logging with 39
- message notifications 46
- servers 40
- service 32
- severity levels 40

syslogd 40

system information 186, 188

## T

TACACS+ authentication method 26, 71

- configuring group authorizations with 84

TACACS+ authentication servers

- configuring in Web Manager 150

talk\_customN.exp Expect script 231

talk\_customN.exp *Expect script* 231

talk\_generic\_ipmi.exp Expect script 231

talk\_rsa\_I.exp Expect script 231, 238

tasks

- basic installation 8
- for assigning a command template to a device 232
- for basic configuration, Wizard 96
- for configuring
  - authentication 27
  - IPSec VPN 72
  - modems 42
  - native IP access 73
  - packet filtering 55
  - power management 44
  - PPTP connections and native IP 73
  - PPTP VPN connections 73
  - SNMP 39
  - syslog 40
  - VPN 70, 73

- not doable using Web Manager 57

Technical support 280

Telnet 31, 32, 82

telnet command 233

terminal 6, 14

Terminal Access Controller Access Control System authentication

- See TACACS+*

terminal blocks 2

terminal emulation program 14

terminal emulator 42

TFTP boot server 277

trap notifications 45

troubleshooting 223–225

- boot image problems 225, 278
- connection methods 223
- network boots and 276
- network failure 223
- understanding boot for 272

type 2 PCMCIA slots 5

## U

U-Boot

- introduction 272
- monitor mode 277

UNIX-based servers 40

unsaved changes

- button 81

username for Cyclades ftp site 191

users 16

- activity, capturing 24
- adding 17
- and groups authorizations 23
- configuring
  - for power management 44

- in Wizard 108
- providing username and password information to 27

- /usr/bin/rmenush login shell
  - configuring 44, 78

## **V**

- virtual IP addresses
  - assigning to a new device 230
  - configuring in Web Manager 106
- virtual network 105
  - configuration in Wizard 103

## **VPN**

- introduction 39–74
- configuration example 254
- configuration tasks 70
- connections
  - IPSec 71
  - PPTP 73

## **W**

- WARNING syslog severity level 40
- Web Manager

- introduction 93–95
  - accessing for configuration 16
  - enabling access 13
  - not displaying OTP authentication 62
  - procedures for enabling access to 14
  - restarting 224
  - to use a dynamic IP address to access 16
  - to use the default IP address to access 16

## **web server**

- Apache 66
  - replacing autogenerated SSL certificate in 66

## **Windows**

- Active Directory server, configuring for group authorizations 84
- Administration Pack, installing 84
  - and PPTP VPN connections 73
  - support for IPSec and PPTP 71

- wire, grounded 12

- Wizard 95–109

- menu options 96

## **X**

- X.509 certificates 71









**Avocent®**

The Power of Being There®

For Technical Support:

[www.avocent.com/support](http://www.avocent.com/support)

Avocent Corporation  
4991 Corporate Drive  
Huntsville, Alabama 35805-6201 USA  
Tel: +1 256 430 4000  
Fax: +1 256 430 4031

Avocent Asia Pacific  
Singapore Branch Office  
100 Tras Street, #15-01  
Amara Corporate Tower  
Singapore 079027  
Tel: +656 227 3773  
Fax: +656 223 9155

Avocent Canada  
20 Mural Street, Unit 5  
Richmond Hill, Ontario  
L4B 1K3 Canada  
Tel: +1 877 992 9239  
Fax: +1 877 524 2985

Avocent International Ltd.  
Avocent House, Shannon Free Zone  
Shannon, County Clare, Ireland  
Tel: +353 61 715 292  
Fax: +353 61 471 871

Avocent Germany  
Gottlieb-Daimler-Straße 2-4  
D-33803 Steinhagen  
Germany  
Tel: +49 5204 9134 0  
Fax: +49 5204 9134 99

590-663-501A