AlterPath™ OnBoard
Installation Guide

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

Release Date: April 2006
Part Number: PAC0390

Contents

Figures

Tables

Procedures

Before You Begin

This *AlterPath OnBoard Installation Guide* provides information and procedures for installing the Cyclades™ AlterPath™ OnBoard and connecting devices.

Audience

This manual is intended for installers of the OnBoard. It provides additional information beyond the simplified installation steps in the *AlterPath OnBoard QuickStart Guide*.

This document describes installation of the OnBoard hardware. It does not describe how to set up and administer other external services or servers that the OnBoard may access for authentication, system logging, IPMI control, SNMP notifications, data logging, file sharing, or other purposes.

Document Organization

The document contains the chapters listed in the following table.

Table P-1: Document Organization

Chapter Number and Title	Description
1: Introduction	Describes the available models, private and public Ethernet ports, LEDs, power options, and all other connections on the AlterPath OnBoard along with necessary prerequisite information for understanding the rest of the information in this guide.

Table P-1: Document Organization (Continued)

Chapter Number and Title	Description
2: Installation	Describes basic installation and lists the contents of the shipping box. Provides procedures for rackmounting the OnBoard, making public Ethernet connections, connecting devices, and enabling Web Manager access.
3: Advanced Installation Topics and Tasks	Describes advanced installation tasks, including how to install a PCMCIA card, connect an external modem or AlterPath PM intelligent power distribution unit (IPDU) to the AUX port.
A. Specifications	Lists the OnBoard's physical specifications, operational features, and certifications.
B. Safety Information	Describes required precautions to follow when installing Cyclades products.
Glossary	Defines terms used when documenting Cyclades products.
Index	Provides page references for terms used in this manual. In the online version, clicking the page numbers in the index brings you to where the terms are used in the manual.

Related Documents

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

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

Table P-2: Related Documents

Guide Title	Printed?	PDFs on Doc CD	Part Number
AlterPath OnBoard QuickStart Guide	Y	Y	PAC0389
AlterPath OnBoard Administrator’s Guide	N (orderable)	Y	PAC0391
AlterPath OnBoard User’s Guide	N (orderable)	Y	PAC0391

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

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

Updated versions of this document will be posted on the downloads section of the Cyclades website when Cyclades releases new versions of the software. See “Additional Resources” on page xv for information about free software upgrades.

Typographic and Other Conventions

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

Table P-3: Typographic Conventions

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

The following table describes other terms and conventions.

Table P-4: Other Terms and Conventions

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

Additional Resources

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

Cyclades Technical Support

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

Cyclades Technical Training

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

Cyclades Software Upgrades

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

See the *AlterPath OnBoard Administrator's Guide* for instructions on upgrading software on your AlterPath OnBoard and on any connected AlterPath PM IPDUs.

Chapter 1
Introduction

This chapter describes the available models, the private and public Ethernet ports, LEDs, power options, and all other connectors on the AlterPath OnBoard and provides additional prerequisite information needed for understanding the rest of the information in this guide

The following table shows the topics covered in this chapter.

OnBoard Connectors

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

- Servers that have service processors with dedicated Ethernet ports
- Other devices that have dedicated Ethernet ports that provide console access.

The following figure illustrates the front of an OnBoard1040 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 Models” on page 4.

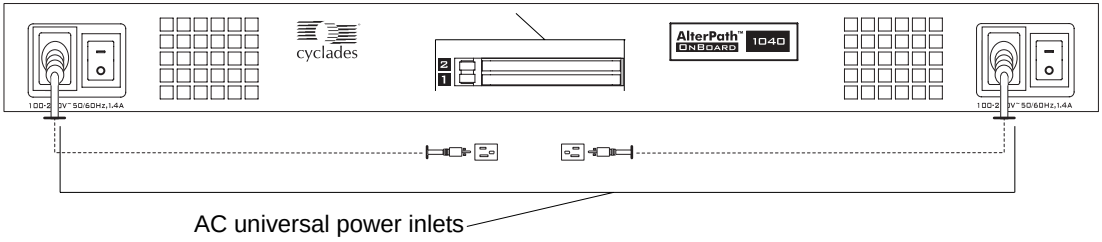


Figure 1-1: OnBoard Front With PCMCIA Card Slots and Two AC Power Inlets

AC models come with either one or two universal power inlets. Customers who purchase AC models chose among a number of different AC power cords to suit the electrical requirements of the region where the unit is being installed.

DC models with two power supplies come with *terminal blocks*, as shown in the following figure. The terminal blocks are for wiring the OnBoard to a DC power source.

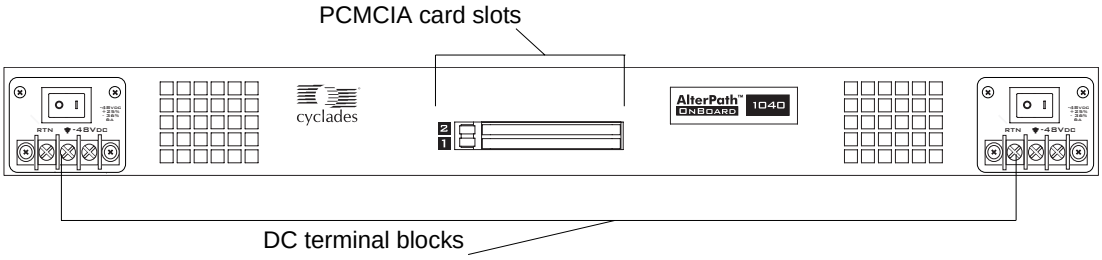


Figure 1-2: OnBoard Front With PCMCIA Card Slots and Two DC Terminal Blocks

The following figure illustrates the back of an OnBoard model that has forty private 10/100 Ethernet ports. (Twenty-four port models are also available, as described in “OnBoard Models” on page 4.)

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.

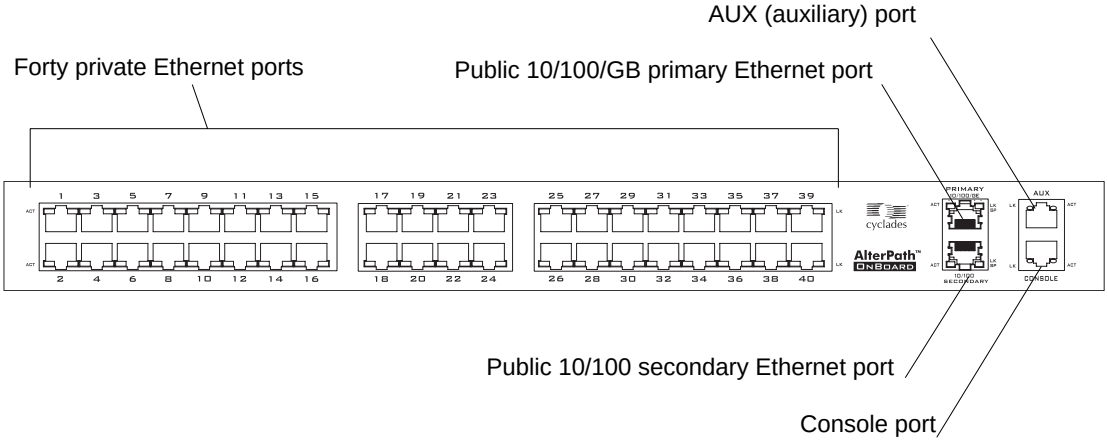


Figure 1-3: OnBoard Back With Ethernet, AUX, and Console Ports

OnBoard Models

Depending on the model, the OnBoard comes with either twenty-four or forty private Ethernet ports. The OnBoard also comes with a variety of power options: either AC power with one or two power supplies or DC power with two power supplies. The following table lists the number and types of power supplies and numbers of public Ethernet ports for each model.

Table 1-1: OnBoard Models

	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

Supported Device Types

The private Ethernet ports on the OnBoard can be connected to the following types of devices:

- A service processor on a server, which has a dedicated Ethernet port
- A blade manager that has an embedded service processor with a dedicated Ethernet port (providing management of multiple internal blades)
- A server or other type of device that does not have a service processor but that provides access to its command line through its Ethernet port. Includes devices that redirect their serial console output to dedicated Ethernet ports.

  Access to a device's console provided by an Ethernet-compatible I/O module is commonly referred to as SoL (serial over LAN).
- A device with a dedicated Ethernet port that supports management access via `telnet`, `ssh`, SNMP, or the OnBoard's native IP access capability.

The OnBoard supports connecting to the types of service processors listed in the following table.

Table 1-2: Types of Service Processors That Work With the OnBoard

Protocol or Access Type	Vendor
IPMI 1.5	Multiple
iLO	Hewlett Packard/Compaq
DRAC III/XT	Dell
RSA II	IBM
Device console	Servers without service processors and other types of devices, such as some routers, that redirect their serial console output to a dedicated Ethernet port

The following types of service processors are not supported by default but may be made to work: IPMI 2.0, RSA-I, RILOE, ALOM. Knowledgeable administrators who need to connect these types of service processors would need to use the `onbdtemplate` utility to find out if new command templates or customized Expect scripts need to be created to handle the interactions. See the *AlterPath OnBoard Administration Guide* for details and contact Cyclades technical support if additional assistance is needed.

The OnBoard has been tested with the above-listed service processors and devices running the specific firmware versions listed in the release notes. If the firmware on a device or service processor being managed by the OnBoard is at another level, the OnBoard administrator can customize command templates. See “Appendix A: Advanced Device Configuration” in the *AlterPath OnBoard Administrator’s Guide.*

See the following figure for an illustration of connecting the OnBoard to a dedicated Ethernet port on a service processor and to another dedicated Ethernet port on a device without a service processor.

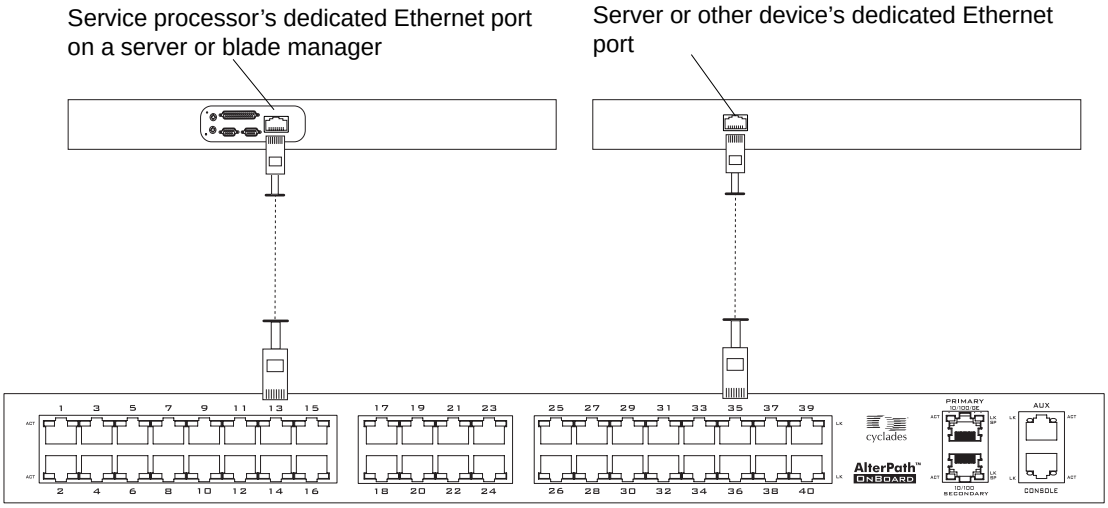


Figure 1-4: Connecting the OnBoard to Devices

After devices are connected to the OnBoard, the administrator must configure the devices as described in the *AlterPath OnBoard Administrator's Guide*.

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.

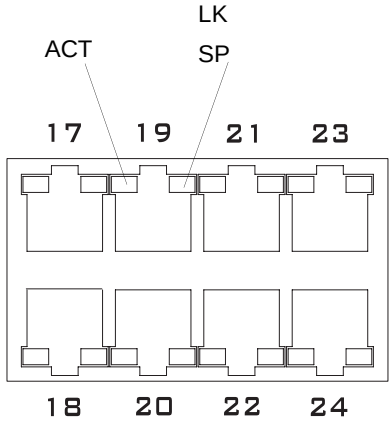


Figure 1-5: LEDs for Private Ethernet Ports

The following figure shows a close up view of the labels on the LEDs on the back right of the OnBoard with numbered callouts. The LEDs in Figure 1-6 monitor the public Ethernet ports, the AUX port, and the console port. The LEDs are described in Table 1-3.

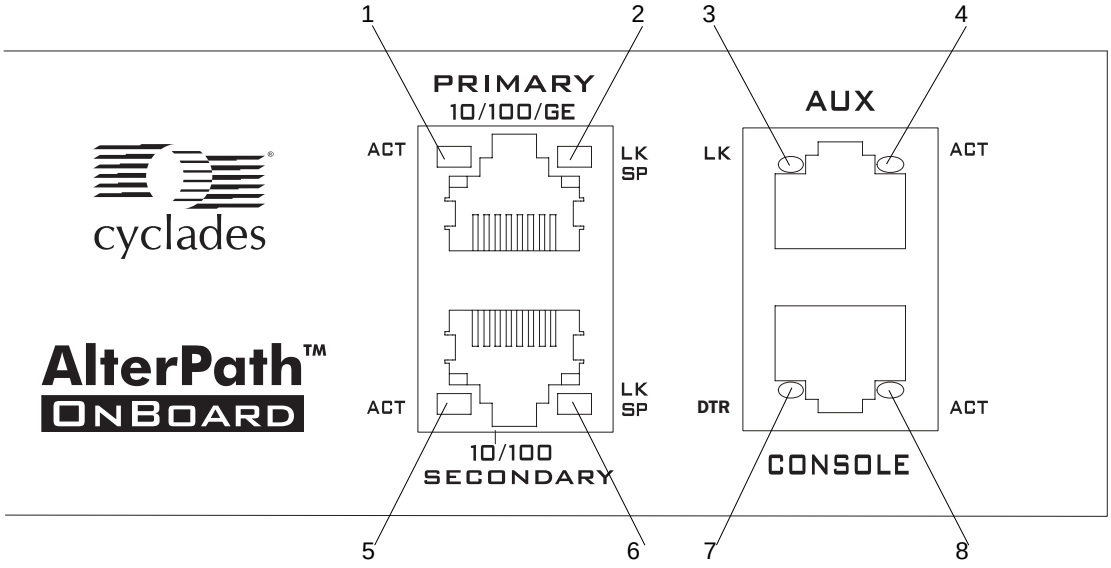


Figure 1-6: LEDs for AUX, Public Ethernet, and Console Ports (Back)

The LED numbers in the table below correspond to the numbers in Figure 1-6.

Table 1-3: LED Descriptions

Number	Label	Function	Color/Status
1,5, and the left LED on all private Ethernet ports	ACT	Monitor Ethernet activity	• 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	• 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	• 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.
4,8	ACT	Monitor RS-232 async activity	• OFF – Indicates no data activity. • Green – Blinks when data is either being received (RX) or transmitted (TX).
7	DTR	Monitors console port for transmissions	• OFF – Indicates OnBoard is not ready to communicate. • ON – Indicates OnBoard is ready to communicate.

PCMCIA Card Slots

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

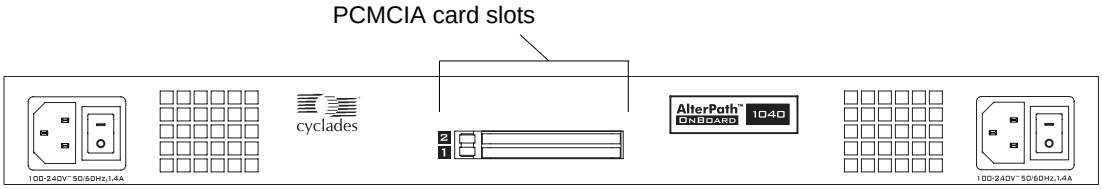


Figure 1-7: PCMCIA Slots on the OnBoard Front

The OnBoard supports the following types of PCMCIA cards:

- 10/100 BaseT Ethernet
- V.9x (56K) Modem
- Compact Flash

The following table shows the supported PCMCIA cards.

Note: Check the AlterPath OnBoard release notes at `http://www.cyclades.com/support/downloads.php` for additional cards that were not yet verified at the time this document was produced. Other PCMCIA cards of the same types shown here possibly work, but they may not have been tested.

Table 1-4: Supported PCMCIA Cards

PCMCIA Card Type	Brand	Model
10/100BT Ethernet	Linksys	EtherFast PCM100 Card Ver.2 and Ver. 3
	CNet	CNF401 Fast Ethernet Cardbus Adapter
V.9x (56k) Modem	Xircom	XM5620 56K PC Card Modem Adapter V.90 Adapter
Compact Flash	Fujifilm	Digital Memory Card 64MB -- CompactFlash

After inserting the PCMCIA card into the OnBoard, the administrator must configure the card as described in the *AlterPath OnBoard Administrator's Guide*.

Modem Types and Options

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

- An external modem can be connected to the AUX port on the back.
- A PCMCIA modem can be inserted into the PCMCIA slots on the front.

The following figure illustrates connecting an external modem to an AUX port and connecting the modem to the telephone network.

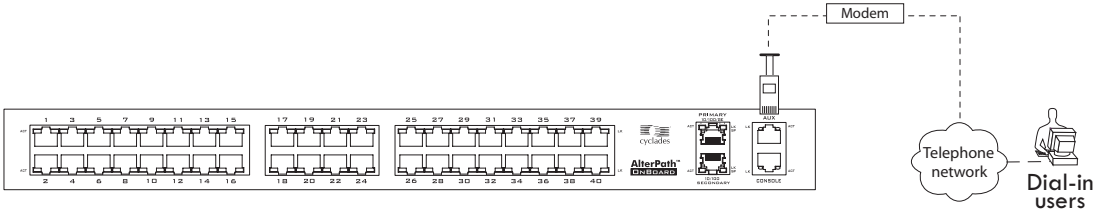


Figure 1-8: Connecting an External Modem to the AUX Port and to the Telephone Network

The following figure illustrates connecting a PCMCIA modem card to the telephone network.

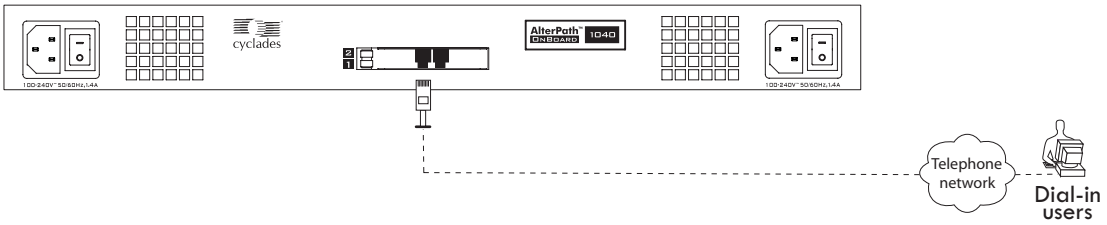


Figure 1-9: Connecting a PCMCIA Modem Card to the Telephone Network

IPDU Power Management Options

AlterPath Power Management (PM) intelligent power distribution units (IPDUs) can be connected to the AUX port on the OnBoard using a RJ-45 to RJ-45 CAT-5 or better cable. Any combination of AlterPath PM models can be daisy-chained to the AUX port to support management of up to a maximum of 128 outlets.

The following figure shows an OnBoard from the back with an IPDU connected to the AUX port and a second and third IPDU daisy-chained from the first IPDU.

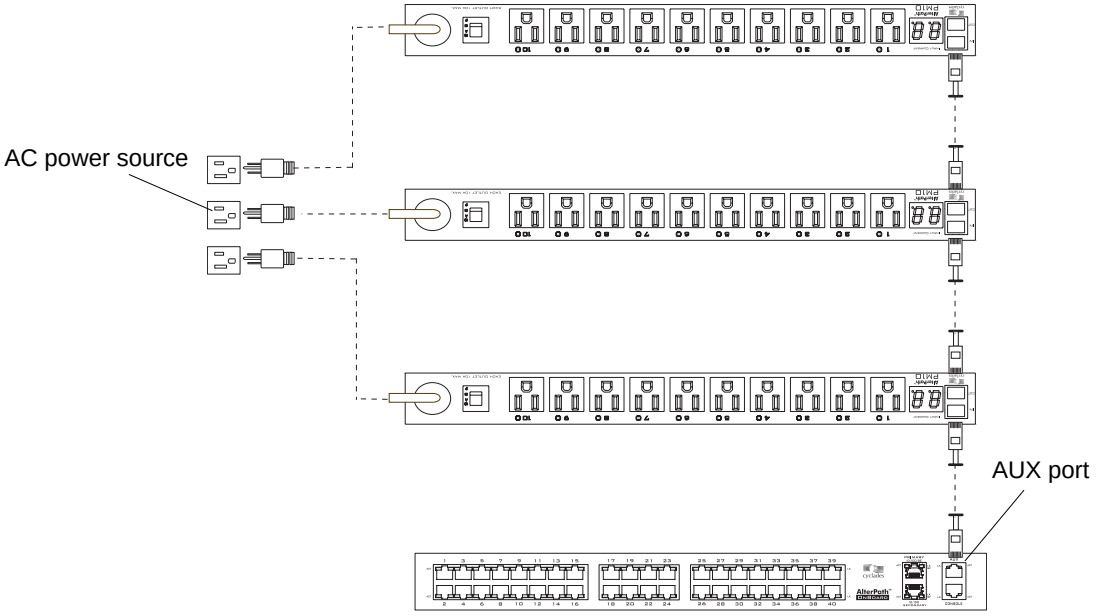


Figure 1-10: IPDUs Daisy-Chained to the AUX Port

After an IPDU is connected to the OnBoard, 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 (as described in the *AlterPath OnBoard Administrator's Guide)*:

- 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 outlets on and off.

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. As illustrated in the following figure, local OnBoard users can access the command line by logging in through the console port.

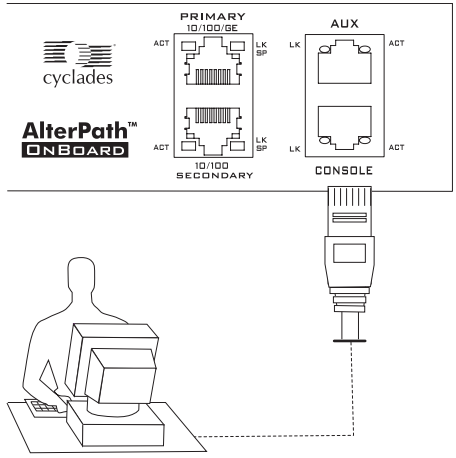


Figure 1-11: User With a Terminal Connected to the Console Port

Authentication Server Options

The administrator chooses a type of authentication to use for accessing the OnBoard and for accessing each connected device, based on the organization's security policy. The installer needs to make sure an authentication server is available for every authentication method used (except for the "Local" authentication method).

The following list summarizes the authentication-related issues for the installer:

- A different authentication method may be specified for accessing the OnBoard than for accessing each connected device.
- The OnBoard must have access to an authentication server set up for every authentication method used.
- Each authentication server must be configured and operational.
- The administrator configuring the OnBoard needs to work with the administrator of each authentication server to get user accounts set up and to obtain usernames, passwords, and other information needed for configuring access to the authentication server on the OnBoard.

For example, if LDAP authentication is to be used for logging into the OnBoard, Kerberos for logins to an IPMI service processor, and RADIUS for logins to a router that has a dedicated Ethernet port, then the OnBoard needs to have network access to an LDAP, a Kerberos, and RADIUS authentication server, and the administrator needs to perform configuration on the OnBoard to enable contact with each type of authentication server.

Chapter 2
Installation

This chapter covers the topics listed in the following table.

The following figure illustrates connections on the front and back as they might appear after the basic installation procedures are completed. (Your connections may be different

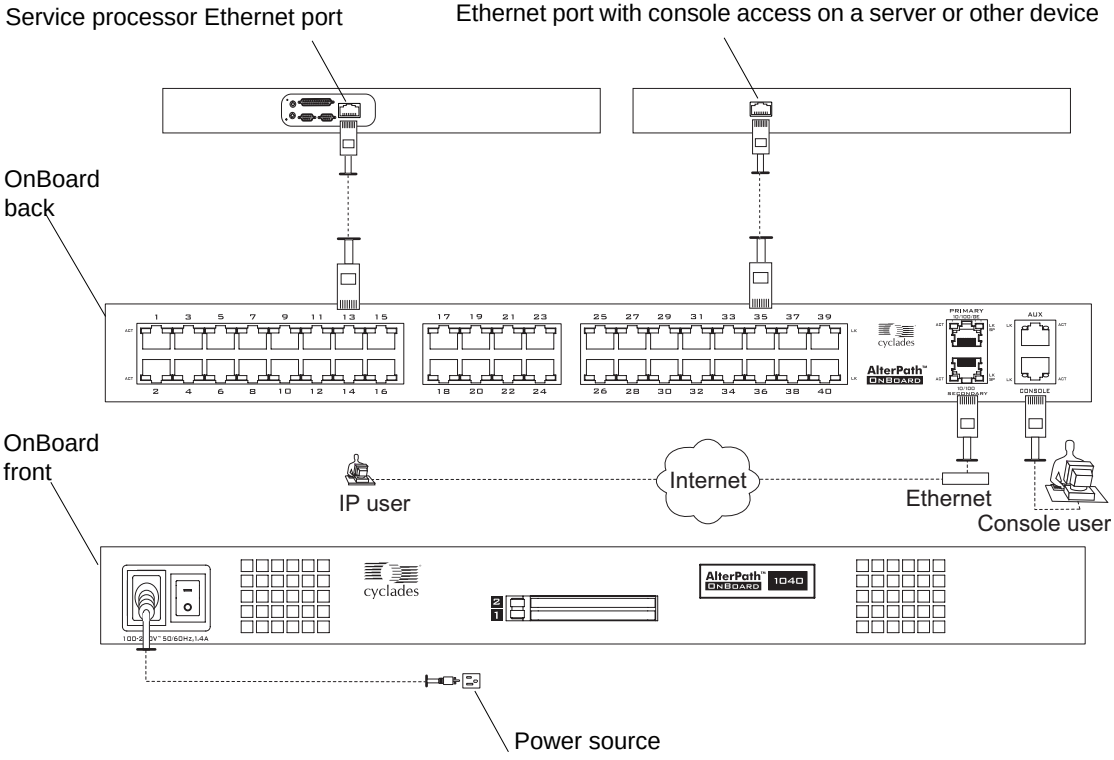


Figure 2-1: Basic Installation Connections Illustrated

Basic Installation Procedures

The following table lists the basic tasks for installing the AlterPath OnBoard and the sections where the tasks are described in more detail.

Note: Before you start installation, make sure you review and follow the safety precautions listed in Appendix B, “Safety Information.”

Table 2-1: Tasks for Basic Installation

Task	Where Documented
Review the contents of the shipping box.	“Shipping Box Contents” on page 18
Rackmount the OnBoard.	“Rackmounting the AlterPath OnBoard” on page 22
Connect the public network to one or both of the public Ethernet ports.	“Making Public Ethernet Connections” on page 23
Connect service processors and other supported devices to the private Ethernet ports.	“Connecting Devices” on page 25
Connect the OnBoard to a power source and turn power on.	“Connecting to a Power Source and Turning On the Power” on page 26
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:	“Methods for Enabling Web Manager Access” on page 29
• To use a connection to the OnBoard’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.	• “Connecting a Terminal to Configure Basic Network Parameters” on page 30 • “To Connect a Terminal to the Console Port” on page 31 • “To Configure Basic Network Parameters Using a Terminal” on page 32
• If using DHCP, discover and use the DHCP-assigned IP address.	• “To Use a Dynamic IP Address to Access the Web Manager” on page 35

Table 2-1: Tasks for Basic Installation (Continued)

Task	Where Documented
• If using the default IP address assigned to the OnBoard, 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.	• "To Use the Default IP Address to Access the Web Manager" on page 35
Select a security profile, add users and configure security and services using the Web Manager.	"Selecting a Security Profile, Adding Users and Configuring Devices Using the Web Manager" on page 37

For how to perform optional advanced procedures [connecting PCMCIA cards, AlterPath PM intelligent power management modules (IPDUs), and external modems], see Chapter 3, "Advanced Installation Topics and Tasks.

Shipping Box Contents

The shipping box contains the AlterPath OnBoard along with the items shown in Table 2-2. The row for each part provides an illustration, its part number (P/N), description, and purpose. You can use checkboxes to check off each item, and you can use the part numbers from this table to reorder any of the parts.

The list is numbered for internal cross-referencing among descriptions within the table.

Table 2-2: Shipping Box Contents, Part Numbers, and Description (Sheet 1 of 4)

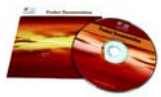
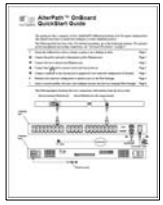
#	Item	P/N	Description	Purpose
1. ☐		PAC0266	Documentation CD	PDF copies of this guide, the OnBoard guides listed in "Before You Begin," and all other Cyclades product documents
2. ☐		PAC0342	*AlterPath OnBoard Quick Start Guide*	Basic installation guide in printed format. Written for expert users experienced in installing Cyclades products.
3. ☐		HAR0608	2 - Mounting brackets with 8 - screws	Use to mount the OnBoard to a rack or cabinet. See "Rackmounting the OnBoard" on page 22.

Table 2-2: Shipping Box Contents, Part Numbers, and Description (Sheet 2 of 4)

#	Item	P/N	Description	Purpose
4. ☐			For AC models, an AC power cable. For DC models, you must wire the OnBoard to your own DC power source. See “To Connect DC Power Terminal Blocks to a DC Power Source and Turn OnBoard Power On” on page 28.	To connect the OnBoard to an AC power source. The standard power for the destination country is used to determine which type of cord is shipped. The ends of available cords are shown in the following rows. Talk with a Cyclades sales representative if the power cable you need is not listed in this table or if you have special requirements.
		CAB0010	NEMA5--15P. Flat blades with round grounding pin.	United States and other countries.
		CAB0037	Schuko. Round pin attachment plug.	European and other countries.
		CAB0055	Oblique flat blades with ground.	Australia, New Zealand, and other countries.

Table 2-2: Shipping Box Contents, Part Numbers, and Description (Sheet 3 of 4)

#	Item	P/N	Description	Purpose
		CAB0056/ CAB0104	Rectangular blade plug.	UK, Ireland, and other countries.
		CAB0278	Flat blades with round grounding pin.	Japan.

Table 2-2: Shipping Box Contents, Part Numbers, and Description (Sheet 4 of 4)

#	Item	P/N	Description	Purpose
5. ☐		CAB0018	RJ-45 to RJ-45 7ft. CAT5 cable	Use for the following: • To connect a public Ethernet port to the LAN. See “To Make a Public Ethernet Connection” on page 24. • To connect a private Ethernet port to a device. See “To Connect Devices to the Private Ethernet Ports” on page 25. • To connect a terminal to a console port. See “To Connect a Terminal to the Console Port” on page 31. • To connect an IPDU or external modem to an AUX ports. See “Connecting One or More IPDUs to the AUX Port” on page 44 and “Connecting an External Modem to the AUX Port” on page 43.
6. ☐		CAB0036	DB-9 female to RJ-45 6 ft. crossover cable	Use to connect the console port or an AUX port to a DB-9 male COM port.

Note: For more information about cabling, see “RS-232 Cabling Tutorial” at http://www.cyclades.com/resources, under “White Papers.” For ordering information, see “Cyclades Product Guide,” available at: http://www.cyclades.com/common/www/pdf/catalog.en.pdf.

1. Rackmounting the AlterPath OnBoard

You can rackmount the OnBoard in a rack or cabinet, mounting it either at the front or the back. Observe all safety precautions described in Appendix B, “Safety Information,” especially making sure to load the rack from the bottom up.

Rackmounting the OnBoard

Before you start, make sure you have the following:

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

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

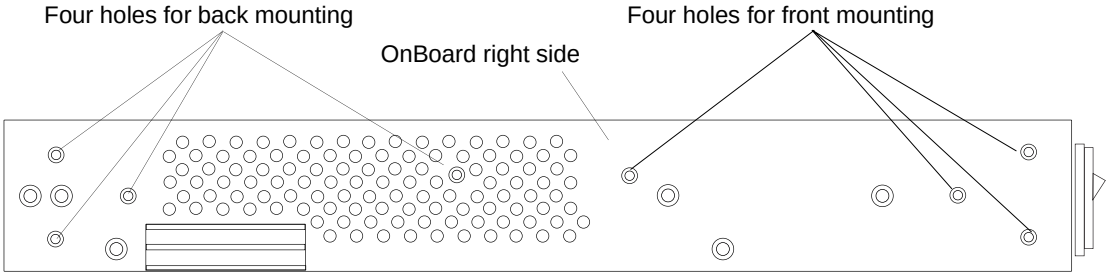


Figure 2-2: Bracket Mounting Holes on the OnBoard’s Right Side

Whether you are front-mounting or back-mounting the OnBoard, you must attach the right bracket to the right side and the left bracket to the left side. The illustration in the following figure shows the left and the right brackets.

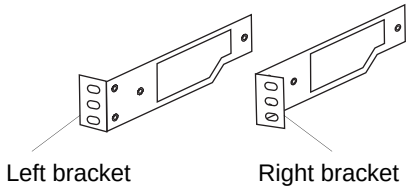


Figure 2-3: Left and right mounting brackets

▼ *To Rackmount the OnBoard*

Prepare the hardware as described under “Rackmounting the OnBoard” on page 22 before you start.

1. Attach the right bracket to the right side and the left bracket to the left side of the OnBoard.
   a. For each bracket, insert fours screws through the holes on the bracket into the appropriate holes at either the front or back of the OnBoard.
   b. Use a Phillips screwdriver to tighten the screws.
2. Use the appropriate mounting hardware to mount the OnBoard to the rails.

2. Making Public Ethernet Connections

The two Ethernet ports on the right back of the OnBoard 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 and remote access to connected devices.

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

- Not used at all
- Used to connect to a second network
- Used 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 administrator needs to enable failover as described in the *AlterPath OnBoard Administrator's Guide*.

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 CAT5 cable shipped with the OnBoard or an off-the-shelf CAT5 or greater cable to connect the Ethernet ports to an Ethernet switch, router, or local area network (LAN) port. The following figure illustrates connecting an RJ-45 connector on one end of a cable to a public Ethernet port on the OnBoard and the other end to a port connecting to the Internet.

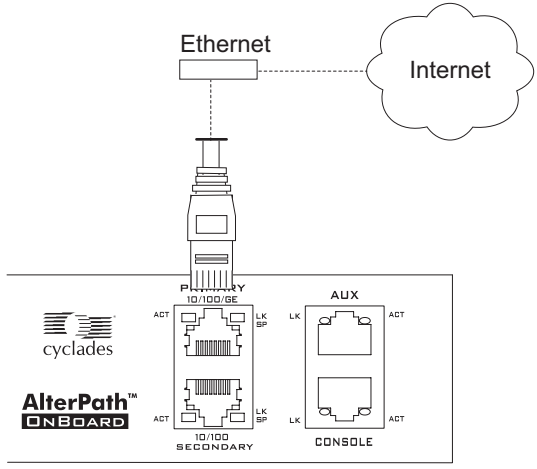


Figure 2-4: Making an Ethernet Connection to a Public Ethernet Port

▼ *To Make a Public Ethernet Connection*

1. Connect one end of a standard Ethernet cable to an Ethernet switch, router, or local area network (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.
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, connect a cable between one of the Ethernet connections listed in Step 1 to the PCMCIA card.

3. Connecting Devices

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

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

Preparing to Connect Devices to the OnBoard

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.

Note: After the OnBoard 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 to any of the following types of Ethernet ports on the other end:
  - A dedicated Ethernet port on a service processor
  - 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 blades' service processors

4. Connecting to a Power Source and Turning On the Power

The OnBoard comes with either one or two power supplies.

When the OnBoard has two power supplies, connect each power supply to a separate power source for redundancy in case one power source fails. For example, connect to one commercial circuit and to one uninterruptible power supply (UPS). The power sources must be independent of each other and must be controlled by separate circuit breakers.

The AC models of the OnBoard have one or two universal power inlets and are shipped with one or two power cords that are appropriate for the region where the OnBoard is to be used. See "To Connect AC Power Inlets to an AC Power Source and Turn OnBoard Power On" for the procedure. The following figure shows an AlterPath OnBoard 1040 with two AC power inlets.

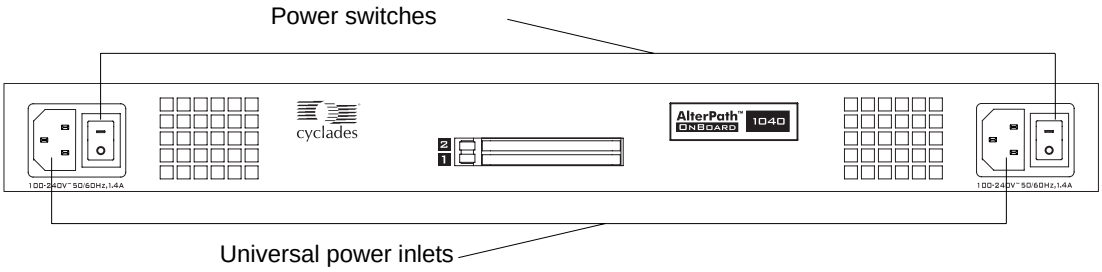


Figure 2-5: Universal AC Power Inlets and Power Switches

The following figure illustrates the same AlterPath OnBoard model as in Figure 2-5 connected to two separate power sources.

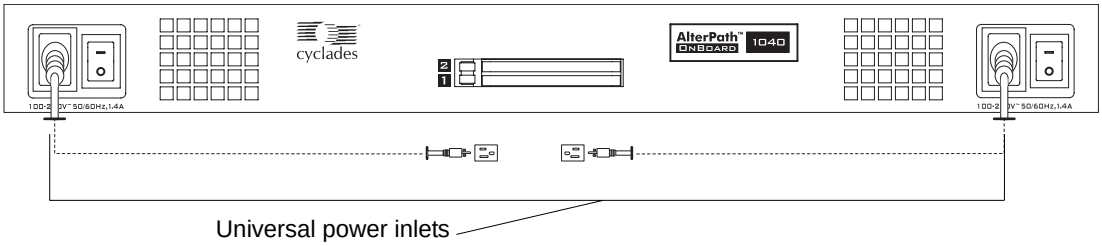


Figure 2-6: Dual AC Model Connected to Two Different Power Sources

The DC models have two terminal blocks, as illustrated in the following figure. Connect the terminal blocks to a DC power source using your own wiring. See "To Connect DC Power Terminal Blocks to a DC Power Source and Turn OnBoard Power On" for the procedure.

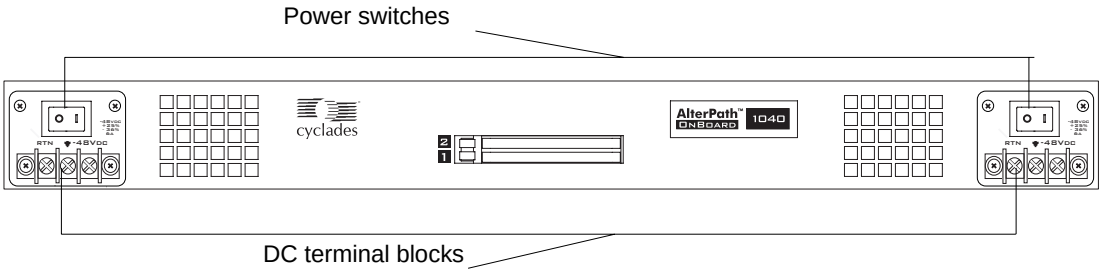


Figure 2-7: DC Model With Two Terminal Blocks

▼ *To Connect AC Power Inlets to an AC Power Source and Turn OnBoard Power On*

1. Make sure the OnBoard's power switch(es) are off.
2. Plug the power cord(s) into the OnBoard 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.

---

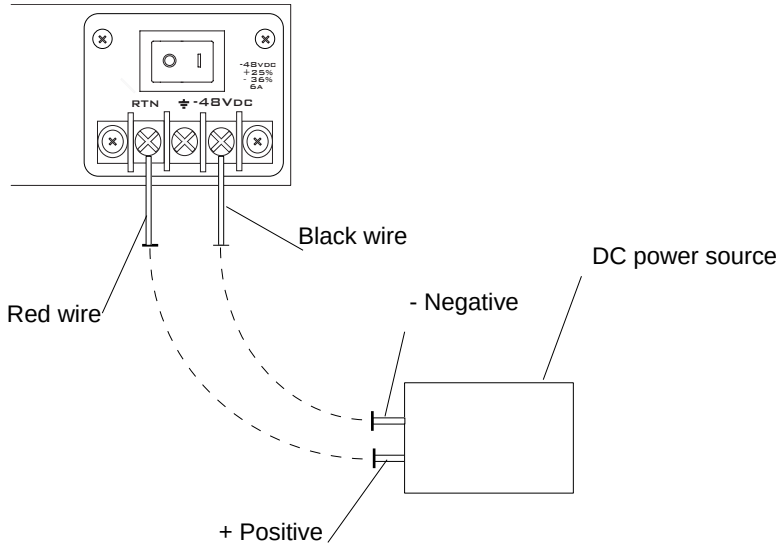
3. Turn the OnBoard's power switch(es) on.

▼ *To Connect DC Power Terminal Blocks to a DC Power Source and Turn OnBoard Power On*

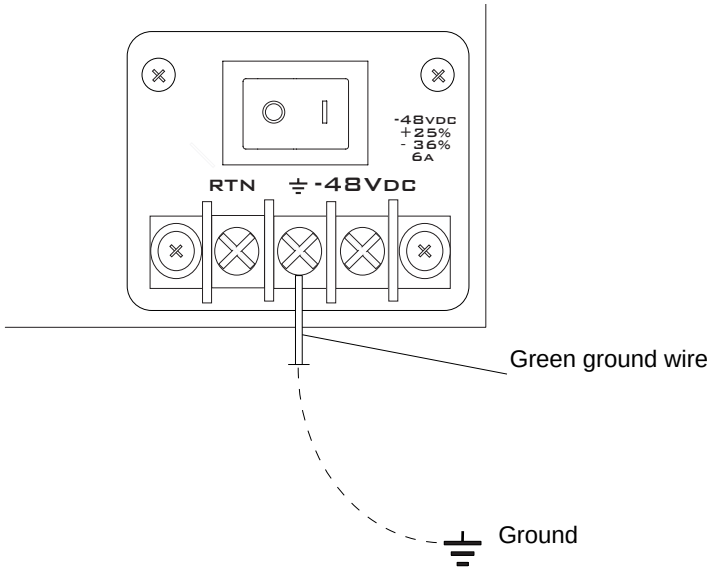
DC models have two *terminal blocks*. You need to connect two screws on each terminal block to a red return wire and a black -48VDC wire from your DC power source, and to connect a third screw from each terminal block to a green ground wire that is grounded either on the power supply or elsewhere.

1. Make sure the OnBoard'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.

      The following figure 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.



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



3. Turn on the OnBoard's power switches.

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 needs to enter the OnBoard'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 2-3: Methods for Enabling Web Manager Access

Method	Considerations	Where Described
Connect a terminal to the console port and use the `cycli` command to assign a static IP address.	You must be at the same location as the OnBoard to make the local connection.	• "Connecting a Terminal to Configure Basic Network Parameters" on page 30

Table 2-3: Methods for Enabling Web Manager Access

Method	Considerations	Where Described
Use the DHCP-assigned address.	DHCP is enabled by default. It relies on a DHCP server that must be available to the OnBoard. a	"To Use a Dynamic IP Address to Access the Web Manager" on page 35
Use the default OnBoard 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.	"To Use a Dynamic IP Address to Access the Web Manager" on page 35

If configuring a static IP address, before you start, collect the following network information from the administrator of the network.

- Hostname: _____
- OnBoard's public IP address: _____
- Domain name: _____
- DNS server's IP address: _____
- Gateway IP address: _____
- Network Mask: _____

If you are using a network time server, obtain the following

- NTP server IP address: _____

5. Connecting a Terminal to Configure Basic Network Parameters

If you connect a terminal or computer 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. The following figure illustrates a computer connection being made to the console port.

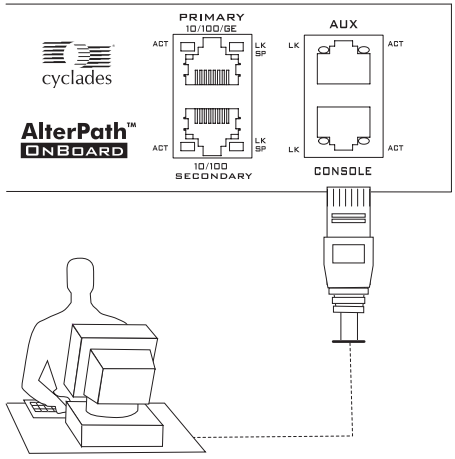


Figure 2-8: Connecting a Terminal to the Console Port

An RJ-45 to DB-9 6 ft. crossover cable is shipped with the OnBoard for the connection. Be sure that whatever cable you use is a crossover cable.

▼ *To Connect a Terminal to the Console Port*

Perform the following steps to connect a terminal or a computer to the console port of the OnBoard. If connecting a PC, ensure that HyperTerminal or another terminal emulation program is installed on the Windows operating system. On a computer 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. CAT5 cable shipped with the OnBoard or an off-the-shelf equivalent CAT 5 or greater cable. If the terminal or other computer has a USB port, you also need a USB to DB-9 converter.

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

a. Connect the RJ-45 end of the cable to the OnBoard'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 computer.

6. Enabling Access to the Web Manager

Perform the procedures in this section to enable a remote administrator to finish configuration using the Web Manager. See Table 2-3, "Methods for Enabling Web Manager Access," on page 29 for details about each method.

▼ *To Configure Basic Network Parameters Using a Terminal*

This procedure requires a terminal or a computer that has a terminal emulation program to be physically connected to the console port of the OnBoard. See "To Connect a Terminal to the Console Port" above.

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

Table 2-4: Terminal Session Settings for Console Port Access

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 root.

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

The default password is "cyclades."

Caution: For security, it is essential for root to change the root password.

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

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

4. Invoke the `cycli` utility.

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

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.

```
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.

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

11. Specify the hostname for the OnBoard.

```
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
active yes
method static
address 192.111.11.111
netmask 255.255.252.0
broadcast 192.111.11.255
gateway none
mtu 1500
```

16. Confirm the name server configuration.

```
cli> get network resolv
dns0 192.111.11.21
dns1 none
domain cyclades.com
```

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 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 are know the IP address that is currently assigned to the OnBoard from a DHCP server on the same subnet.

1. Use the OnBoard's dynamically-assigned IP address in a browser to bring up the Web Manager.

2. Finish configuring users and to the OnBoard using the Web Manager.

3. Make sure that the root user changes the password by logging into the OnBoard console.

See "To Change Root's Password" on page 36.

▼ *To Use the Default IP Address to Access the Web Manager*

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

1. On a computer that has a physical network connection to the OnBoard, change the network portion of the IP address of that computer to `192.168.160` and make sure that the host portion of the IP address is not the same as the OnBoard's.

For example, you could change the computer's IP address to `192.168.160.44`. For the host portion of the IP address, you can use any number except `10`, `0`, or `255`

2. Bring up a browser on the computer whose address you changed, enter the OnBoard'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 computer, go to the Wizard "Network Settings" option to change the OnBoard's IP address to a fixed public IP address and to configure the other basic network parameters.
4. Restore the computer's IP address to its previous IP address.
5. Make sure that the root user changes the root password by logging into the OnBoard console.

   See "To Change Root's Password" on page 36.

Changing Root's Password

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

- Until an IP address is available for the OnBoard, the only way that root can change the root password is to log in locally through the console port.

  See Step 1 "To Configure Basic Network Parameters Using a Terminal" on page 32.
- After an IP address is available for the OnBoard, the remote root user can use `ssh` to connect to the OnBoard 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'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
```

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

For the configuration tasks the administrator needs to perform, see the *AlterPath OnBoard Administrator’s Guide*. These tasks include selecting a security profile, adding users, and configuring devices.

For how OnBoard administrators and regular users access the OnBoard and perform device management actions on connected devices, see the *AlterPath OnBoard User’s Guide*.

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

Chapter 3
Advanced Installation Topics and Tasks

This chapter covers the advanced procedures listed in the following table.

Installing PCMCIA Cards in the Front Card Slots

See Table 1-4 on page 9 for a list of supported PCMCIA cards.

Order of installation is important, as described here:

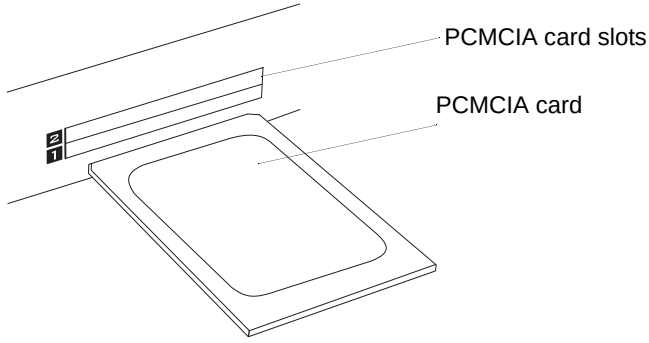
- Two PCMCIA cards of different types can be installed in any order.
- Two PCMCIA cards of the same type must be installed in the following order:
  - Insert and configure the first card in slot 1.
  - Insert and configure the second card in slot 2.

Swapping in 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 42 to remove any existing cards, insert and configure the new card and reinsert and reconfigure the old card.

▼ *To Install a Single 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. See the *AlterPath OnBoard Administration Guide* for configuration details for supported PCMCIA card types.

▼ *To Install Two PCMCIA Cards*

1. If both cards are of different types, install and configure both cards in any order.

See the procedure in "To Install a Single PCMCIA Card" on page 40 if needed.

2. If the cards are of the same type, insert and configure the first card in slot 1 before inserting and configuring the second card in slot 2, as in the following steps:

a. Insert a card into slot 1.

b. Configure the card in slot 1. (See "To Install a Single PCMCIA Card" on page 40.)

c. Insert a card into slot 2.

d. Configure the card in slot 2.

▼ *To Remove a PCMCIA Card*

1. On the Web Manager → Settings → PCMCIA form, press the Eject button next to the card's slot number.

2. On the front of the OnBoard, press the button next to the PCMCIA slot.

3. Physically remove the card from the slot.

▼ *To Swap In a New PCMCIA Card*

1. Do these steps if all the following are true:
   - Only one card slot is in use
   - The new card is the same type as the one already installed in the slot
   - You want to replace the card in the current slot.

   a. Eject the card.

      See “To Remove a PCMCIA Card” on page 41, if needed.

   b. Insert and configure the new card.

      See “To Install a Single PCMCIA Card” on page 40 if needed.

2. If all the following are true, insert the new card into the empty slot and configure the new card:
   - Only one card slot is in use
   - The new card is the same type as the one already installed in the slot
   - You want to add the new card into the empty slot

   See “To Install a Single PCMCIA Card” on page 40 if needed.

3. If both card slots are in use, do the following steps:

   a. Eject the card.

      See “To Remove a PCMCIA Card” on page 41, if needed.

   b. Press the buttons next to both PCMCIA slots on the front of the Insert and configure the new card.

      See “To Install a Single PCMCIA Card” on page 40 if needed.

Connecting an External Modem to the AUX Port

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

The following figure illustrates connecting an external modem to an AUX port and connecting the modem to the telephone network.

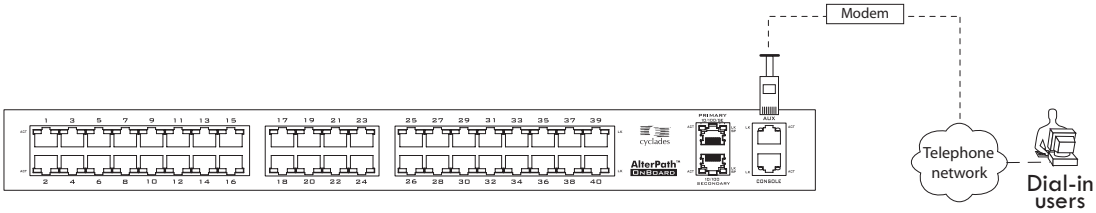


Figure 3-1: Connecting an External Modem to the AUX Port and to the Telephone Network

▼ *To Connect an External Modem to the AUX Port*

This procedure requires the following cables and connectors:

- A straight through CAT5 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 adapter (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.

1. Connect the RJ-45 end of the cable to the AUX port on the OnBoard.
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 the *AlterPath OnBoard Administrator's Guide* for details about configuring the AUX port.

Connecting One or More IPDUs to the AUX Port

You can daisy-chain any combination of AlterPath PM intelligent power distribution units (IPDUs) to the AUX port with up to a total of 128 outlets.

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

The following figure shows an OnBoard from the back with an IPDU connected to the AUX port and a second and third IPDU daisy-chained from the first IPDU.

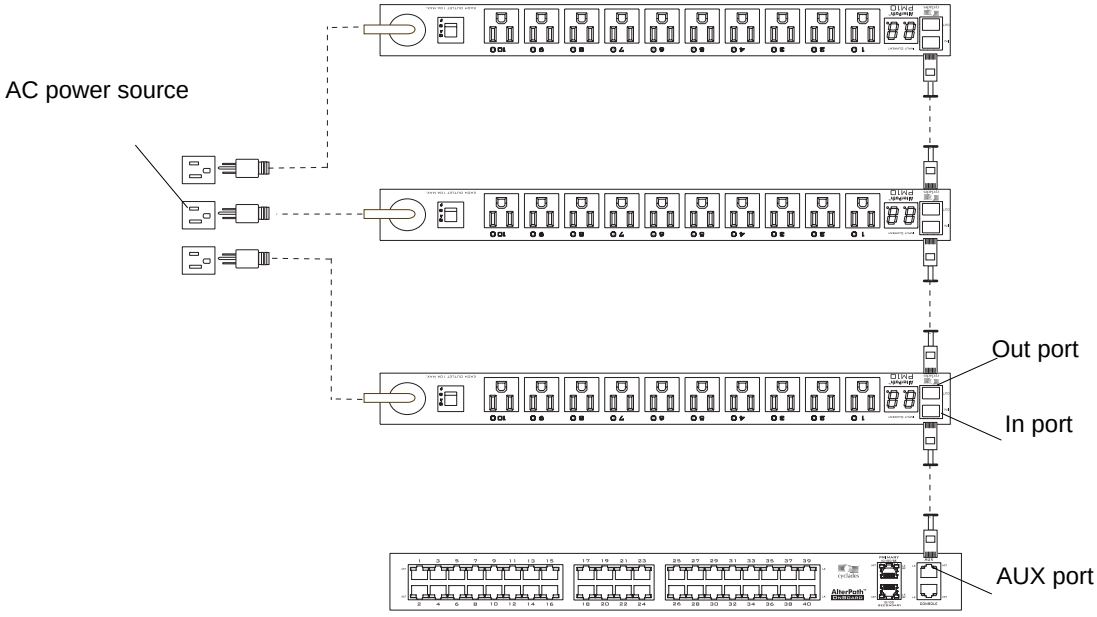


Figure 3-2: IPDUs Daisy-Chained to the AUX Port

▼ *To Connect an IPDU to the AUX Port*

You need a straight-through RJ-45 to RJ-45 CAT5 or greater cable for connecting the AlterPath PM IPDU.

1. Connect one end of the cable to an AUX port on the OnBoard.
2. Connect the other end of the cable to the "In" port of the AlterPath PM.

If you are daisy-chaining additional PMs, go to “To Daisy-Chain AlterPath PMs to the OnBoard” on page 45.

3. Configure the AUX port for Power Management.

   See the *AlterPath OnBoard Administrator’s Guide* for details about configuring the AUX port.

▼ *To Daisy-Chain AlterPath PMs to the OnBoard*

This procedure assumes that one AlterPath PM is connected to the AUX port on the OnBoard. You need a straight-through RJ-45 to RJ-45 CAT5 or greater cable for each AlterPath IPDU PM you will be connecting.

1. Connect one end of a CAT5 cable to the “Out” port of a AlterPath PM that is already connected to the AUX port of a OnBoard.
2. Connect the other end of the CAT5 cable to the “In” port of the next AlterPath PM.
3. Repeat Steps 1 and 2 until you have connected the desired number of AlterPath PMs.
4. Configure the AUX port for Power Management.

See the *AlterPath OnBoard Administrator’s Guide* for details about configuring the AUX port, and for how to make sure that all daisy-chained PMs are running the same firmware version.

A
Specifications

Tables in this appendix list the physical specifications for the OnBoard along with its operating features and certifications.

Physical Specifications

The following table lists the OnBoard's physical specifications.

Table A-1: Physical Specifications

CPU	Freescale Power QUICC III
Memory	256 MB DDRAM/128 MB compact flash
Interfaces	24/40 Ethernet 10/100 BT on RJ-45 1 RS-232 console on RJ-45 1 RS-232 DTE on RJ-45 for power manager or external modem 1 10/100/10000 BT Ethernet on RJ-45 for primary user connections 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: • Ethernet • Dial-up modem • Flash memory
Dimensions (WxDxH)	17 in x 12 in x 1.75 in 43.18 cm x 80 cm x 4.45 cm
Operating Temperature	50° F to 122° F 10° C to 50° C
Storage Temperature	-40° F to 185° F -40°C to 85° C
Humidity	5% to 90% noncondensing
Enclosure	Steel

Table A-1: Physical Specifications (Continued)

Power	Universal AC, single or dual 100-240 VAC • 50/60Hz • 1.4 A max Dual DC • 36 to 75 VDC • 5 A max input current

Operating Features

The following table lists the OnBoard's operating features.

Table A-2: Operating Features

Operating system	Linux
Security	SSHv1 and SSHv2
	Authentication: Local, RADIUS, TACACS+, LDAP, NIS, OTP, Active Directory/NTLM, and Kerberos
	Local fallback user authentication [in case of remote failure]
	Group authentication from authentication servers
	System event logs
	VPN through PPTP or IPSec
User Interface	Web Manager (HTTP/HTTPS)
	Configuration wizard for first time configuration
	Command line interface (Linux shell)
	OnBoard-specific management commands
	SNMP
	Security profiles for quick setting of security features (turning services on and off)
	NTP for time server synchronization
	Optional integrated power management with the AlterPath PM
	Support for service processor management software from most server vendors

Table A-2: Operating Features (Continued)

Service Processor Management	Simultaneous access to multiple service processors
	Support for service processor console redirection (remote KVM)
	Serial console over LAN
	Restricted user access to power, sensors, console, event logs, or native IP access type applications
	DHCP for dynamic or fixed IP address assignment
	Support for proprietary service processors
Upgrades/Network Boot Option	Software and documentation upgrades posted for download on public FTP site
	Upgradeable flash
	TFTP support for network boot

Standards and Certifications

The following table lists the OnBoard's applicable standards and certifications.

Table A-3: 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

Table A-3: Standards and Certifications (Continued)

Country/Region	Standards and Certifications	Scope
European Union	CE mark relevant directives	EMC directive: • EN55022: 1998 + A1:2000, Class A Emission Information Technology Equipment—Radio Disturbance Characteristics—Limits and methods of measurement (CISPR 22:2203, + A1:2004) • EN55024: 1998 + A1:2001, Immunity Requirements Information Technology Equipment—Immunity Characteristics—Limits and methods of measurement (CISPR 24:1997 + A2:2002) Safety Directive: • EN60950-1:2001 Information Technology Equipment—Safety—Part 1: General Requirements
USA	Federal Communications Commission (FCC)	FCC Part 15 Class A

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

B
Safety Information

Follow the precautions in this appendix when installing Cyclades 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. See Appendix A, “Specifications” on page 47 for specific standards and compliance information for the AlterPath OnBoard.

General Safety Precautions

Observe the following general safety precautions when setting up and using Cyclades 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.
- Chose 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 a Cyclades 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 Cyclades 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 Cyclades 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.

Glossary

1U

One rack unit (also referred to as 1RU). A standard measurement equal to 1.75” (4.45 cm) of vertical space on a rack or cabinet that is used for mounting computer equipment.

3DES

Triple Data Encryption Standard, an encrypting algorithm (cipher) that encrypts data three times, using a unique key each time, to prevent unauthorized viewers from viewing or changing the data. 3DES encryption is one of the *security features* provided by Cyclades products to enable customers to enforce their data center security policies. See also *authentication*, *authorization*, and *encryption*.

ActiveX

A set of technologies developed by Microsoft from its previous OLE (object linking and embedding) and COM (component object model) technologies. Browsers used for accessing KVM output from devices connected to Cyclades AlterPath KVM products must have ActiveX enabled.

advanced lights out manager (See *ALOM*)

AH (*authentication header)*

One of the two main protocols used by IPSec. (*ESP* is the other.) AH authenticates data flowing over the connection. AH is not compatible with *NAT*, so it must be employed only when the source and destination networks can be reached without NAT. Does not define the authentication method that must be used.

alias

An easy-to-remember, usually-short, usually-descriptive name used instead of a full name or IP address. For example, on some Cyclades products, port names contain numbers by default (as in Port_1) but the administrator can assign an alias (such as *SunBladeFremont* that describes which server is connected to the ports. Aliases make it easier for users to understand which devices are connected.

ALOM (advanced lights out manager)

A service processor on certain Sun servers that includes an independent system controller and firmware. Provides remote monitoring, logging, alerting, and basic control of the server.

application-specific integrated circuit (See *ASIC*)

ASIC (Application-Specific Integrated Circuit)

Pronounced “ay-sik”. A type of chip used for applications that provide a specific function, such as an ASIC chip that serves as a *BMC*.

authentication

The process by which a user’s identity is checked (usually by checking a user-supplied username and password) before the user is allowed to access requested resources. Authentication may be done locally (on the Cyclades device) or on a configured authentication server running one of the widely-used authentication protocols (LDAP, RADIUS, TACACS+, NIS, SMB, and Kerberos) that are supported by Cyclades products. Authentication is one of the *security features* provided on Cyclades products to enable customers to enforce their data center security policies. See also *authorization* and *encryption*.

authentication header (See *AH)*

authorization

Permission to access a controlled resource, which must be granted by administrative action. A user’s authorizations are checked after a user logs into a system and has been authenticated. Each user is restricted to using only the features the user is authorized to access. Checking a user’s authorizations

is one of the *security features* provided on Cyclades products to enable customers to enforce their data center security policies. A user who is authorized to access a device or software function is referred to as an *authorized user.* See also *authentication* and *encryption*.

authorized user

One who is given permission to access a controlled resource, which must be granted by administrative action.

backup configuration

On Cyclades products, specifies where to save compressed configuration files for possible later restoration. Some Cyclades products save configuration changes in the affected configuration files while maintaining a backed-up compressed set of configuration files in a separate directory. The backup directory's contents are available for restoration until the administrator takes a specific action to overwrite the backed-up files.

baseboard

A gender-neutral term for "motherboard."

baseboard management controller (See *BMC*)

basic input/output system (See *BIOS*)

baud rate

Pronounced "bawd rate." When configuring terminal or modem settings on serial ports and console port connections on AlterPath devices, the specified baud rate must match the baud rate of the connected devices.

Options range from 2400–921600 bps. 9600 is the most-common baud rate for devices.

BIOS (basic input/output system

Pronounced “bye-ose.” Instructions in the onboard flash memory that start up (boot) a computer without the need to access programs from a disk. Sometimes used for the name of the memory chip where the start-up instructions reside. BIOS access is available even during disk failures. Administrators often need to access the BIOS while troubleshooting, for example, to temporarily change the location from which the system boots in case of a corrupted operating system kernel. How to access the BIOS varies from one manufacturer to the other.

BMC (baseboard management controller)

An internal processor on some servers that is separate from the main system and that operates even if the main processor is not operable. Sits on the server’s baseboard (motherboard), on an internal circuit board, or on the chassis of a blade server. Monitors on-board instrumentation. Provides remote reset or power-cycle capabilities. Enables remote access to BIOS configuration or operating system console information. In some cases provides *KVM* control of the server. Includes a communication protocol that delivers the information and control to administrators.

bonding

See *Ethernet bonding*.

callback

A *security feature* used to authenticate users who are calling into a device. The software authenticates the user, hangs up, and then returns the call to the user before allowing access.

CAT5 (category 5)

A standard for twisted-pair Ethernet cables defined by the Electronic Industries Association and Telecommunications Industry Association (commonly known as EIA/TIA).The support for CAT5 and later cabling (such as CAT5e) in many Cyclades products allows the use of existing cabling in the data center.

CDMA (code division multiple access)

A mobile data service available to users of CDMA mobile phones.

CHAP (challenge handshake authentication protocol)

An authentication protocol used for PPP authentication. See MS-CHAP.

checksum

Software posted at the Cyclades download site is accompanied by a checksum (`*.md5`) file generated using the MD5 algorithm. The checksum of a downloaded file must be the same as the checksum in the file. The checksum is compared automatically when the download is performed through the Web Manager or can be compared manually if the download is performed using `ftp` or `http`. If the checksums do not match, the software file is damaged and should not be used.

CLI (command line interface)

Allows users to use text commands to tell computers to perform actions (in contrast to using a GUI). The user types a text command at an on-screen prompt and presses the Enter or Return key. The computer processes the command, displays output when appropriate, and displays another prompt. Users can save a series of frequently-used commands in a script. Being able to create and run scripts to automate repetitive tasks is one of the reasons many administrators prefer using a CLI.

Cyclades products run the Linux operating system, and most Cyclades products allow access to the command line of the Linux shell. Command line access is achieved through several different means. For one example, a remote administrator can use Telnet or SSH to access an AlterPath OnBoard and then can enter commands on the Linux shell's command line.

Some Cyclades products offer a management utility called the CLI. Administrators type “CLI” or “cli” at the prompt in the Linux shell. Products that provide similar utilities with different names, such as the AlterPath OnBoard `cycli`, provide an alias for users who are familiar with the CLI name. The Cyclades CLI tool provides many commands and nested parameters in a format called the *CLI parameter tree*.

CLI parameter tree

Each version of the Cyclades *CLI* utility has a set of commands and parameters nested in the form of a tree. The CLI for the AlterPath OnBoard and other products use the Cyclades Application Configuration Protocol (CACP) daemon (cacpd). The cacpd uses the `param.conf` file, which defines a different CLI parameter tree for each product.

client-side management software—See *management software*

command line interface (See *CLI*)

community name

A string used as a type of shared password by *SNMP* v1 and v2 to authenticate messages. Hosts that share the same community name usually are physically near each other. The administrator must supply a community name when configuring SNMP on the Cyclades device, and the same community name must be also configured on the SNMP server. For security reasons, the default community name *public* cannot be used.

console

A computer mode that gives access to a computer's command line (see *command line interface*). The console also displays error messages generated by the computer's operating system or *BIOS*. Console access is essential when a device (such as some special-purpose servers, routers, service processors, and other embedded devices) has no window system. Console access is also essential when the window system is not available on a device that has one, either because the system is damaged or it is offline. Access to the console allows remote administrators to control and repair damaged or otherwise-unavailable systems. See also *device console* and *service processor* console.

console servers

Appliances that give consolidated access to the console ports of connected assets, either over the network, through dial-in, or direct serial connection.

Cyclades

A corporation founded in 1989 to provide unique networking solutions. Named after the ground-breaking French packet-switching network created in 1970, which was named after the Greek province of Cyclades. Cyclades in Greece is made up of many islands that when viewed on a map resemble a diagram of nodes in a computer network.

decryption

Decoding of data that has been encrypted using an *encryption* method.

Dell Remote Assistant Cards (See *DRAC*)

Dell Remote Administrator Controller (See *DRAC*)

device console

The console on a server or another type of device that allows access to its console through an Ethernet port that is connected to one of the OnBoard's private Ethernet ports.

DHCP (dynamic host configuration protocol)

A service that can automatically assign an IP address to a device on a network, which saves administrator's time and reduces the number of IP addresses needed. Other configuration parameters may also be managed. A DHCP server assigns a dynamic address to a device based on the *MAC address* of the device's Ethernet card. Many Cyclades devices are shipped with DHCP client software, and with DHCP enabled by default.

dial-in

A method of connecting to a remote computer using communications software, such as *PPP*, along with a modem, and a telephone line, which is supported on many Cyclades products. After the administrator of the Cyclades product has connected a modem from the Cyclades product to a live telephone line and made the phone number available, a remote authorized user can use the phone number to dial into the Cyclades product and access connected devices.

DNS (domain name service or system)

A service that translates domain names (such as `cyclades.com`) to network IP addresses (192.168.00.0) and that translates host names (such as "onboard") to host IP addresses (192.168.44.11). To enable the use of this service, administrators need to configure one or more DNS servers when configuring AlterPath devices.

DRAC (Dell Remote Access Controller)

All of the following combinations are used for defining this acronym, with multiple definitions appearing even at the Dell website: Dell Remote [Access | Administrator | Administration] [Controller | Card].

Service processors on certain Dell servers may include an independent DRAC system controller. Several incompatible version types exist (DRAC II, DRAC III, DRAC III/XT, DRAC IV) along with several incompatible firmware versions. All controller types have a battery and can have an optional PCMCIA modem installed. Provide remote monitoring, logging, alerting, diagnostics, and basic control of the server. Some types have a *native web interface* and a *native application* "Dell OpenManage Server Administrator," that runs on the remote administrator's computer. Dell Open ManageIT Assistant software on the administrators computer can be used to configure and launch access.

The OnBoard provides access to many but not all DRAC management functions on supported DRAC versions. To access all the management functions available through DRAC requires *native IP* access.

encapsulating security payload (See *ESP*)

encryption

Translation of data into a secret format using a series of mathematical functions so that only the recipient can decode it. Designed to protect unauthorized viewing or modification of data, even when the encrypted data is travelling over unsecure media (such as the Internet). See 3DES and SSH. As an example, a remote terminal session using secure shell SSH usually encrypts data using 3DES or better algorithms. Encryption is one of the security features provided on Cyclades products to enable customers to enforce their data center security policies. See also *authentication* and *authorization*.

ESP (encapsulating security payload)

One of the two main protocols used by IPSec (*AH* is the other). ESP encrypts and authenticates data flowing over the connection. Does not define the authentication method that must be used. DES, 3DES, AES, and Blowfish are commonly used with ESP.

Ethernet bonding

Synonymous with *Ethernet failover.* A way of configuring two Ethernet ports on a single device with the same IP address so that if the primary Ethernet port becomes unavailable, the secondary Ethernet port is used. When bonding is enabled, the active IP address is assigned to bond0 instead of eth0. When the primary Ethernet port returns to active status, the software returns it to operation.

Ethernet failover

See *Ethernet bonding*. See also *failover.*

event log

Referred to as the system event log (SEL) on most service processors, a timestamped record of events such as power on/off, device inserts/removals/ connects/disconnects, sensor threshold events and alerts.

Expect script

A script written using `expect`, a scripting language based on Tcl, the Tool Command Language. Can be written to perform automation and testing operations that are not possible with other scripting languages. Cyclades uses `expect` scripts in some of its AlterPath products, and users can customize some of the default expect scripts. For example administrators of the AlterPath OnBoard can customize the Expect scripts that handle conversations with service processors and other supported devices.

failover

A high-availability feature that relies on two redundant components in a system or a network, with the second component available to automatically take over the work of the primary components if the primary component becomes unavailable for any reason. When the primary component becomes available, it takes over the work again. Automatically and transparently redirects requests from the unavailable component to the backup component. Used to make systems more fault-tolerant. See *Ethernet bonding*.

flash memory

A chip used to store the operating system, configuration files, and applications on some Cyclades products.

GPRS (general packet radio service)

A mobile data service available to users of GSM mobile phones that adds packet data capabilities.

GSM (global system for mobile communications)

Originated by the GSM (Groupe Special Mobile) group in France in 1982. A popular standard for mobile phones.

GUI

Graphical user interface (pronounced GOO-ee). A computer interface that allows users to tell computers to perform actions by clicking on graphical elements such as icons, choosing options from menus, and typing in text fields on forms displayed on the computer screen. Many Cyclades products provide GUI access through the Cyclades Web Manager.

HTTP (hypertext transfer protocol)

Protocol defining the rules for communication between Web servers and browser across the Internet.

HTTPS (secure HTTP over SSL)

Protocol enabling the secure transmission of Web pages by encrypting data using *SSL* encryption. URLs that require an SSL connection start with `https`.

IETF (Internet Engineering Task Force)

Main standards organization for the Internet. Working groups create Internet Drafts that may become RFCs. RFCs that are approved by the Internet Engineering Steering Group (IESG) may become standards. RFCs (Requests for Comments) are the official technical specifications of the Internet protocol suite. For example, the format of *SNMP MIBs* was defined by the IETF, which assigns MIB numbers to organizations.

iLO (Integrated Lights Out)

Hewlett Packard's proprietary service processor (pronounced *EYE-loh*). Even though HP is a major supporter of IPMI, the company also provides iLO because it provides many more functions than IPMI. The iLO processor resides on the *baseboard*. Even if the server is off, iLO is active. When the dedicated Ethernet port is plugged into the network, iLO uses DHCP. iLO has a web interface and a Telnet interface. Advanced iLO provides remote KVM and *virtual media* access.

integrated lights out (See *ILO*)

IP address consolidation

Provides controlled access to basic management features on multiple Ethernet-based servers that have embedded service processors, using only one Internet address. When managed separately, each service processor needs its own IP address. Managing multiple servers with multiple IP addresses is both expensive and time consuming without consolidation.

IPDU (intelligent power distribution unit)

A device with multiple power inlets into which IIT assets can be plugged for remote power management. Cyclades supports a family of AlterPath PM IPDUs that can be remotely managed when they are connected to AlterPath devices, such as the AlterPath KVM/net or AlterPath OnBoard.

IPMI (Intelligent Platform Management Interface)

An open standards vendor-independent service processor currently adopted by many major server platform vendors. Its main benefit over other service processor types is that it is installed on servers from many vendors, providing one interface and protocol for all servers. Its main disadvantage is that it does not always provide as much functionality as the proprietary service processors. For this reason, IBM's series e325 and e326 servers use IPMI to manage their BMCs but the top-of-the-line xSeries servers use *RSA II*. IPMI works by interacting with the *BMC*, and since it usually has standby power, it can function even if the operating system is unavailable or if the system is powered down. The OnBoard supports IPMI version 1.5. OnBoard administrators can create custom *Expect* scripts to support IPMI 2.0.

ipmitool

A command line utility that interfaces with any *BMC* that supports either IPMI 1.5 or 2.0 specifications. Reads the sensor data repository (SDR) and prints sensor values, displays the contents of the System Event Log (SEL), prints Field Replaceable Unit (FRU) inventory information, reads and sets LAN configuration parameters, and performs remote chassis power control. Described at SourceForge at: `http://ipmitool.sourceforge.net`. The command options are described on the `ipmitool`(1) man page at SourceForge: `http://ipmitool.sourceforge.net/manpage.html`. `ipmitool` commands can be added to customized scripts on the OnBoard to access unsupported features on a connected service processor.

IPSec (Internet protocol security)

A suite of protocols used for establishing private, secure, connections over IP networks. Only the sending and receiving computers need to be running IPSec. Each computer handles security at its end and assumes that the intermediary nodes between the source and destination computers are not

secure. Supported on many AlterPath products. In tunnel mode, IPSec is used to form a *VPN* connection, creating a secure tunnel between either an individual host or a subnet on one end and the AlterPath device on the other end. Has two modes, *transport* and *tunnel* mode. Tunnel mode encrypts the entire packet. Transport mode encrypts application headers, TCP or UDP headers, and packet data, but not the IP header. The method that encrypts the entire packet cannot be used where NAT is required

Kerberos

Network *authentication* protocol designed to provide strong authentication for client/server applications by using secret-key cryptography.

KVM

Remote keyboard, video [monitor], and mouse access to a server through a PS/2 or USB connection on a server that is connected to a KVM switch.

KVM analog switch

A *KVM switch* that requires a local user connection before a user can gain access to any servers that are connected to the switch. Cyclades AlterPath KVM analog switches are one component of the *out-of-band infrastructure*.

KVM over IP switch

A *KVM switch* that supports remote access over a LAN or WAN or telephone line to servers connected to the switch, using the TCP/IP protocols and a web browser. Enables operations over long distances. Cyclades AlterPath KVM/IP switches are one component of the *out-of-band infrastructure*.

KVM switch

Enables use of only one keyboard, video monitor, and mouse to run multiple servers from a remote location. Reduces expenses by eliminating the cost of acquiring, powering, cabling, cooling, managing, and finding data-center space for one keyboard, monitor, and mouse for every server. Servers are connected to KVM ports on Cyclades AlterPath KVM switches using AlterPath KVM terminators on the server end and up to 500 feet of *CAT5* or greater cable. AlterPath KVM switches provide *authentication* and other *security features* and allow only *authorized users* to access a restricted set of connected servers. See also *KVM analog switch* and *KVM over IP switch*.

Cyclades AlterPath KVM analog switches are one component of the *out-of-band infrastructure*.

LDAP (lightweight directory access protocol)

A directory service protocol used for authentication. One of many standard authentication protocols supported on Cyclades devices.

MAC address

Also called the Ethernet address. A number that uniquely identifies a computer that has an Ethernet interface. Cyclades equipment displays MAC addresses on a label on the bottom.

management console—See service processor

management network

A network separated from the *production network* that provides remote *out-of-band* access for management of IT assets, including access for returning disconnected IT assets to service without the need for a site visit.

management software

Each server company that offers a service processor produces its own client-side software to access the servers' management features through the service processor. In some cases, management software is imbedded in the service processor and is presented either as a web interface or as a command line interface accessed using SSH or Telnet, or as both a web interface and command line interface. In other cases, the management software is installed in a client workstation and accesses the management features of the service processor using an IP-based protocol, such as *IPMI*. Most of these types of software only manage one server, do not scale, and do not address the need for consolidated access-control, multi-user access, data logging, and event detection, encyrption and other needs. The OnBoard addresses these needs and provides a single interface to access basic features of multiple-vendors' service processors.

MIB

Each *SNMP* device has one or more MIBs (management information bases), which describes the device's manageable objects and attributes. The MIB name tree for Cyclades starts at 1.3.6.1.4.1.4413.

MIIMON

A value set when configuring Ethernet failure to specify how often the active interface is inspected for link failures. A value of zero (0) disables MII link monitoring. A value of 100 is a good starting point, according to SourceForce bonding documentation.

MS-CHAP (Microsoft challenge handshake authentication protocol)

The Microsoft version of CHAP, which does not require the storage of a clear or reversibly-encrypted password. Can be used with or without AAA (authentication, authorization, and accounting). If AAA is enabled, PPP authentication can be done by TACACS+ and RADIUS.

NAT

Network address translation, an Internet standard that enables the use of one set of IP addresses for internal traffic and another set of IP addresses for traffic over the public network. The AlterPath OnBoard uses NAT to allow access to service processors and managed devices while not revealing their Ethernet addresses. Users can use administratively-assigned virtual IP addresses to access the service processor or device through the OnBoard.

native applications

A management option that gives the user the ability to run *service processor*-specific *native applications* and access the application's management features from the user's remote computer through the OnBoard. For example, the IBM service processor provides the IBM Director native application.

To obtain this type of access, the authenticated and authorized user selects the "Native IP" option after establishing a VPN connection between the user's computer and the OnBoard. At that point, the user can bring up the management application from where it resides on the user's computer or on the service processor and use the service processor's server management functions.

n*ative command interface* (See *NCI*)

native IP

A management option that the OnBoard administrator can enable when configuring a *service processor*. Because this option provides full access to all features supported by the service processor, the user must be a trusted user who is specifically authorized to use the option. A *VPN* connection must be made before the user is allow to access the native IP option. When the OnBoard user activates Native IP for a service processor, the OnBoard routes packets between that user's IP address and the service processor through a secure tunnel. The VPN connection must remain active for the duration of the Native IP session. Authorizing a user for native IP gives the user access to a *native application* or a *native web interface* that may be provided by the service processor and that may provide additional management functions beyond those provided by the OnBoard, including *KVM over IP* access to the server.

native web interface

A service processor feature that allows browser access to the service processor's information, management, configuration, and actions, by means of a HTTP/HTTPS server running on the service processor. Access to this feature requires the user to be authorized for *native IP*.

NCI (native command interface)

A *service processor* feature that allows direct access to the *console* of the service processor. Access may be provided to features such as power control, hardware auditing, event logs, sensor readings, and service processor configuration, usually by means of a Telnet or *SSH* server running on the service processor.

NEBS (Network Equipment Building System) Certification

Means that equipment has been tested and proven to meet the NEBS requirements for central office equipment that is adhered to in common by several telecommunications carriers. The requirements are in place to ensure that telecommunications equipment poses no risk or safety hazard to people, nearby equipment, or to the physical location where the equipment operates, and that equipment is reliable and dependable during both normal and abnormal conditions. Tests address heat release, surface temperature, fire

resistance, electromagnetic capability, electrical safety, and manufacturing component characteristics, among other attributes.

network time protocol (See *NTP*)

netmask

The dotted-decimal expression that determines which portion of an IP address represents the network IP address and which is used for host IP addresses, for example, 255.0.0.0.

NIS (Network Information Service)

A directory service protocol used for authentication in UNIX systems. One of many standard authentication protocols supported on Cyclades devices.

NTLM (NT LAN manager)

An authentication protocol used by Microsoft *SMB*.

NTP (network time protocol)

A protocol used to synchronize the time in a client with a high-accuracy network time protocol server.

OID

A unique indentifier for each object in an *SNMP MIB*. The OID naming scheme is in the form of an inverted tree with branches pointing downward. The OID naming scheme is governed by the IETF, which grants authority for parts of the OID name space to individual organizations. Cyclades has the authority to assign OIDs that can be derived by branching downward from the node in the MIB name tree that starts at 1.3.6.1.4.1.4413.

SNMP programs use the OID to identify the objects on each device that can be managed by using SNMP.

onbdshell

The OnBoard shell, `/usr/bin/onbdshell`, which displays a menu of devices an authorized user can access. Accessed by authorized users through selecting the “Access Devices” option from the user shell menu, *`rmenush`*. Selecting a server name from the menu brings up the list of actions the user is

authorized to perform on that server's *service processor.* Accessed by administrators by typing`/usr/bin/onbdshell` on the OnBoard's command line; the administrators' version of the menu lists all configured devices.

OOBI (Out-of-band Infrastructure)

An integrated systems approach to remote administration. Consists of components that provide secure, *out of band* access to connect to and manage an organization's *production network*. Components can include console servers, KVM and *KVM over IP* switches, power control appliances, centralized management devices (to control the entire out-of-band infrastructure), and service-processor managers to manage access to multiple vendor's service processors. Allows administrators to remotely connect to disconnected IT assets and to quickly return them to normal operation. Cyclades AlterPath products are designed as building blocks for an OOBI, including AlterPath ACS console servers, AlterPath KVM and KVM over P switches, AlterPath OnSite with consolidated console and KVM ports, AlterPath PM IPDUs, the AlterPath OnBoard service- processor manager, and the AlterPath Manager for centralized control of and access through multiple AlterPath devices to up to 5000 connected devices, and for access to servers that have IPMI controllers.

OTP (one-time passwords)

An authentication system that requires the user to generate and use a new password for every connection. The OTP can only be used once, which ensures that a discovered password is useless. Originally developed at Bellcore (now Telcordia), it started as a freely available program called S/Key that was trademarked. A newer freeware OTP program is OPIE (one time passwords in everything).

out of band

Access to IT assets that is either separate from or independent of the normal *production network.* A term that originated in the telecommunications industry to refer to communications used to control a phone call that are made on a dedicated channel, which is separate from the channel over which the call is made. Allows remote monitoring and control even when a managed IT asset loses connection to the production network. Typically, out-of-band access is through a *console* or management port (typically an RS-232 or Ethernet port),

an *intelligent power management device* (IPDU), a *KVM* port, or a *service processor.*

point to point protocol (See *PPP*)

point to point tunneling protocol (See *PPTP*)

PPP (point to point protocol)

A method that creates a connection between a remote computer and a Cyclades device and enables a remote user access using the Web Manager or the command line. Supports the use of the PAP, SPAP, CHAP, MS-CHAP, and EAP authentication methods.

PPTP (point to point tunneling protocol)

A *VPN* method developed by Microsoft along with other technology companies, it is the most widely supported VPN method among Windows clients and the only VPN protocol built into Windows 9x and NT operating systems. Uses the same types of authentication as PPP.

production network

The network on which the primary computing work of an organization is done. Users on a production network expect 24/7/365 availability with access to data and resources as reliable as access to telephone service. Development and testing of new applications are often performed on separate networks to avoid burdening or compromising the production network. Organizations often set up separate *management networks* to provide remote *out-of-band* access to disconnected IT assets.

RADIUS (remote authentication dial in user service)

A widely-supported authentication protocol for centralized user administration. Used by many Internet Service Providers (ISPs) and by devices such as routers and switches that do not have much storage. Combines authentication and authorization in a user profile. Relies on the UDP protocol. One of many standard authentication protocols supported on Cyclades devices.

remote supervisor adapter II (See *RSA II*)

remote system control (See *RSC*)

rmenush

The default login shell for users (`/usr/bin/rmenush`), which allows users only a limited set of menu options, including: access to management actions on devices for which they are authorized; the ability to change the user's password; and the ability to logout. The OnBoard administrator may modify the menu options and commands.

RSA II (remote supervisor adapter II)

Service processor technology on certain IBM servers that includes a service processor PCI card used to manage the BMC that is located on the motherboard. Enables the remote administrator to receive notifications, alerts, to view event logs and the last screen before a failure, to use virtual media (also called "remote media"), to control power and to manage the console through a web browser using a built-in Web server. Provides more options than the IPMI service processor that is available on IBM xseries e325 and e326 servers.

RSC (remote system control)

Service processor technology on certain Sun servers that includes a *service processor* RSC card. Enables the remote administrator to run diagnostic tests, view diagnostic and error messages, reboot the server, and display environmental status information from a remote console even if the server's operating system goes offline. The RSC firmware runs independently of the host server, and uses standby power drawn from the server. The RSC card on some servers include a battery that provides approximately 30 minutes of power to RSC in case of a power failure.

secure rack management (See *SRM*)

security features

Cyclades products provide security features, including *encryption*, *authentication*, and *authorization*, to enable customers to enforce their data

center security policies while providing *out-of-band* access to managed systems.

SEL (See *event log*)

serial over LAN (See SoL)

service processor (See SP)

service processor console

The console on a service processor whose dedicated Ethernet port is connected to one of the OnBoard's private Ethernet ports. Sometimes referred to as NCI (for native command interface). [OnBoard only]

service processor manager

An *OOBI* component that provides to users and groups secure, controlled access to basic features required for out-of-band management of servers that have embedded management controllers (also called *BMC*s or *service processors*). Also provides access to the console of servers and other devices without service processors but that have Ethernet ports that allow console access. Provides a single point of access through a single Ethernet address (see *IP address consolidation*) to services that are provided by service processors from several different vendors and to the console of certain servers and other devices. Its administrators are able to use a single interface to manage multiple servers without having to learn multiple management interfaces. The AlterPath OnBoard is the Cyclades service processor manager.

shell

A command interpreter on UNIX-based operating systems (like the Linux operating system that controls most Cyclades products). A shell typically is accessed in a terminal window where the shell presents a prompt. For example: `[admin@OnSite admin]#` is the prompt that appears when a user logs into an OnSite as admin and is in the `/home/admin` directory. Users tell the operating system to perform actions by typing commands in the shell, which interprets the commands and performs the specified actions. See also *command line interface*. The AlterPath OnBoard has two user shells: `onbdshell` and `rmenush`.

simple mail transfer protocol (See *SMTP*)

SMB (server message block)

A protocol used for file sharing and other communications between Windows computers. Microsoft uses this protocol along with NTML authentication protocol used to authenticate a client on a server.

SMTP (simple mail transfer protocol)

The most-commonly-used protocol used to send email.

SNMP (simple network management protocol)

A set of network management protocols for TCP/IP and IPX (Internet Packet Exchange) networks, which are part of the TCP/IP protocol suite. Supports management of devices running SNMP agent software by remote administrators using *SNMP manager software*, such as HP OpenView, Novell NMS, IBM NetView, or Sun Net Manager, on remote computers. Devices running SNMP agent software send data from management information bases (*MIBs*) to the SNMP manager software.

On certain Cyclades devices, administrators can enable SNMP to allow a remote administrator to manage the device and can configure the device to send alerts about events of interest. Before enabling SNMP, the administrator needs the following information: The contact person (administrator) of the AlterPath device; the physical location, the *community name* (for SNMP v1, v2c only), IP address or DNS hostname of the *SNMP manager*. The OnBoard supports SNMP v1, v2c, and v3. The SNMP configuration file is located at `/etc/snmp/snmpd.conf`. See also *OID* and *traps*.

SNMP manager

Any computer running SNMP manager software. Also called a network management station or SNMP server.

SNMP manager software

Displays data about managed devices on the console or saves the data in a specified file or database. Some network management programs such as HP OpenView graphically show information about managed devices.

SNMP server (See SNMP manager)

SoL *(*serial over LAN)

Access to the console of a server or other device that supports redirection of serial server data to a dedicated Ethernet port. Permits access to and control of the BIOS and operating system console over the LAN or Internet. Eliminates the need for the device to have a serial port and the need for serial cabling to enable console access. On the OnBoard, once a device's SoL Ethernet port is connected to one of the OnBoard's private Ethernet ports, an authorized user can access the server or a device's console either through the "Device console" or "devconsole" option (available on the *Web Manager*, `rmenush`, or `onbdshell`) or through entering the `devconsole` command with `ssh` on the command line).

SP (service processor)

Ethernet-based management controller on a server, which provides out-of-band management through an interface between the server's administrator and an internal baseboard management controller (BMC) that enables the management features. Management features can include serial console emulation (using Telnet or IPMI), *KVM over IP,* power control, sensor and log information from the server hardware, and virtual media.

SRM (secure rack management)

An out-of-band infrastructure (OOBI) capability delivered by the AlterPath OnBoard that isolates the management ports (emergency service ports) of servers that have *service processors* from the *production network*. Physically consolidates and logically secures the Ethernet connections between the AlterPath OnBoard and the connected service processors. By providing *IP consolidation*, SRM substantially lowers the cost and complexity of deploying service processors. SRM also lowers the security risks of using service processors by providing centralized authentication and user access control, isolating vulnerable service processor protocols from the production network and communicating with authenticated and *authorized users* over the public network using higher-end secure protocols (such as *SSH*, *SSL*, and *HTTPS*).

SSH

Secure shell, developed by SSH Communications Security, Ltd., is a UNIX-based *shell* and protocol that provides strong authentication and secure communications over unsecured channels. Unlike `telnet`, `ftp`, and the `rcp`/`rsh`/`remsh` programs, SSH encrypts everything it sends over the network. Many Cyclades products support SSH version 1 and SSH version 2. Since SSH1 and SSH2 are entirely different, incompatible protocols, it is important when given a choice between enabling one or the other of the two SSH versions to enable the version that is available on the computer being used to access the Cyclades equipment. The OpenSSH (`www.openssh.org`) package is used on the AlterPath OnBoard. THe OnBoard uses the Open SSH version that is certified by the Cryptographic Module Validation (CMV) program run by the U.S. National Institute of Standards (NIST) and the Canadian government's Communications Security Establishment (CSE). Authorized users on the AlterPath OnBoard can enter an OnBoard-specific set of commands such as poweron, poweroff, powercycle when using `ssh` on the command line to perform *service processor* management actions.

SSL (secure sockets layer)

A protocol for transmitting private documents via the Internet. Also used for the type of connection used for transmitting the information. Uses two keys to encrypt data being transferred: a public key and a private or secret key known only to the message receiver. See also *HTTP/HTTPS*.

system event log (See *event log*)

TACACS+ (Terminal Access Controller Access Control System)

An authentication protocol (pronounced *tak-ak_plus*) that provides separate authentication, authorization, and accounting services. Based on TACACS, but completely incompatible with it. Uses the TCP protocol, which is seen by some administrators as a more-reliable protocol than the UDP protocol used by RADIUS. One of many standard authentication protocols supported on Cyclades devices.

trap

An operation started by an SNMP agent in response to an event of interest on a managed-object in a device, which sends an alert to the *SNMP manager*. The administrator of certain Cyclades device can configure which types of events generate trap messages and trap destinations. Also known as SNMP messages or as “PDUs”—protocol data units.

virtual media

Emulates the use of a floppy or CD drive that is physically connected to the remote administrator’s computer to

VPN (virtual private network)

A mechanism enabling two computers to securely transfer information over an otherwise untrusted network through a secure tunnel. Two common options used for VPN are *IPSec* and *PPTP*.

Web Manager

Cyclades' web management interface. The Web Manager runs in supported browsers and allows remote administrators to configure Cyclades products and to enable remote users to access servers and other devices that are connected to Cyclades products. Authorized users can use the Web Manager to access connected devices.

Index

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W

X