AlterPath™ OnSite
Installation Guide

Software Version 1.1.0

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: May 2006
Part Number: PAC0463

Contents

Figures

Tables

Procedures

Before You Begin

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

Audience

This manual is intended for installers of the OnSite. It provides additional information beyond the simplified installation steps in the *AlterPath OnSite QuickStart Guide*, including important safety requirements.

This document describes installation of the OnSite hardware. It does not describe how to set up and administer other external services or servers that the OnSite 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, the KVM and serial ports, LEDs, power options, and all other connectors on the AlterPath OnSite along with providing 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 OnSite, making an Ethernet connection, connecting servers and other devices, and enabling Web Manager access for further configuration by the administrator.
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 an AUX port.
A. Specifications	Lists the OnSite'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 OnSite.”

The following table lists the AlterPath OnSite documents. As indicated, the QuickStart Guide is printed and is also included with the other AlterPath OnSite 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 OnSite.”

Table P-2: Related Documents

Guide Title	Printed?	PDFs on Doc CD	Part Number
AlterPath OnSite QuickStart Guide	Y	Y	PAC0342
AlterPath OnSite Administrator’s and User’s Guide	N (orderable)	Y	PAC0464

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 xvii 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 OnSite 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 OnSite or for an AlterPath PM that you may also be using with this product.

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

Chapter 1
Introduction

This chapter describes the available AlterPath OnSite models, the KVM and serial ports, LEDs, and all other connectors on the AlterPath OnSite and provides additional prerequisite information needed for understanding the rest of the information in this installation guide.

The following table shows the topics covered in this chapter.

OnSite for Installers

The OnSite is a 1U device that serves as a single access point for the following purposes:

- Accessing servers and other devices that may be connected to its KVM and serial ports
- Managing power through optionally connected AlterPath PM IPDUs.

Depending on the model, the OnSite comes with either four or eight KVM ports and four or eight serial ports, for connecting the following devices:

- From four to eight servers with KVM connections

AND

- From four to eight devices of either of the two following types connected to serial ports:
  - Devices with console ports, such as switches, routers, PBXs, or headless servers
  - Dumb terminals that can launch `telnet`, `ssh`, or raw socket sessions on remote servers

The following figure illustrates the front of an OnSite.

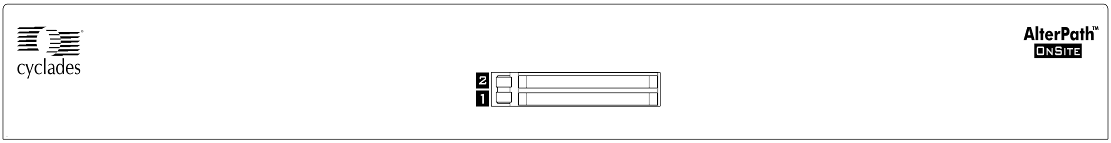


Figure 1-1: OnSite Front

The following figure shows the back of the OnSite.

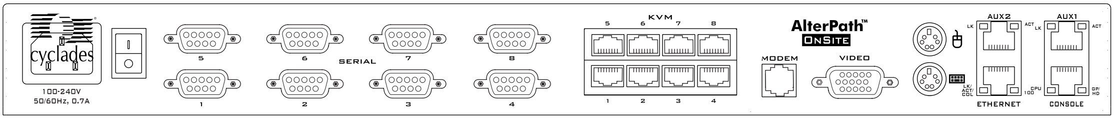


Figure 1-2: OnSite Back With Connectors

Overview of Connectors on the OnSite

The following table describes the types of connectors on the OnSite.

Table 1-1: OnSite Connectors and Intended Uses

Connector	Description
Serial ports	DB-9 serial port connectors for connecting: • Servers and other devices that have console ports • Dumb terminals Allows the use inexpensive off-the-shelf cables.
KVM ports	RJ-45 connectors that accept RJ-45 to RJ-45 CAT5 or greater cables, which plug into AlterPath KVM terminators, which are connected to servers VGA (monitor), keyboard, and mouse connectors.
Modem port	RJ-11 jack for connecting the internal modem to an active telephone line for dial-in access to the internal V.92 56Kbps modem. (Does not rely on the IP network being up.)
Video, [mouse], [keyboard]—KVM connectors	PS/2 and VGA ports for connecting a *Local User station* (keyboard, monitor, and mouse).
Console	An RJ-45 port for connecting the OnSite by means of a RJ-45 to DB-9 or DB-25 CAT5 or greater cable to a COM port either on a terminal or on a computer running a terminal emulator (for local administration)
AUX 1 and AUX 2	RJ-45 ports that can be used for the following: • Connecting to an optional external modem • Connecting to an optional CSU/DSU device **Note:** Modem and CSU/DSU devices allow dial-in access through the AUX ports. • Connecting to an optional AlterPath PM IPDU or to multiple daisy-chained IPDUs.

Table 1-1: OnSite Connectors and Intended Uses (Continued)

Connector	Description
Ethernet	An RJ-45 port for connecting to an Ethernet network for Intranet and Internet access. Both 10BaseT and 100BaseT Ethernet speeds are supported.
PCMCIA card slots	Type 2 PCMCIA card slots for inserting cards that provide additional access and storage options, including dial-in access through modem or phone cards.

Connectors on the Back

The back of the OnSite has KVM, serial, and management ports, a power cord connector, and a power switch.

The following figure shows the back of the OnSite with its serial, KVM, modem, Local User, auxiliary (AUX), Ethernet, and console ports.

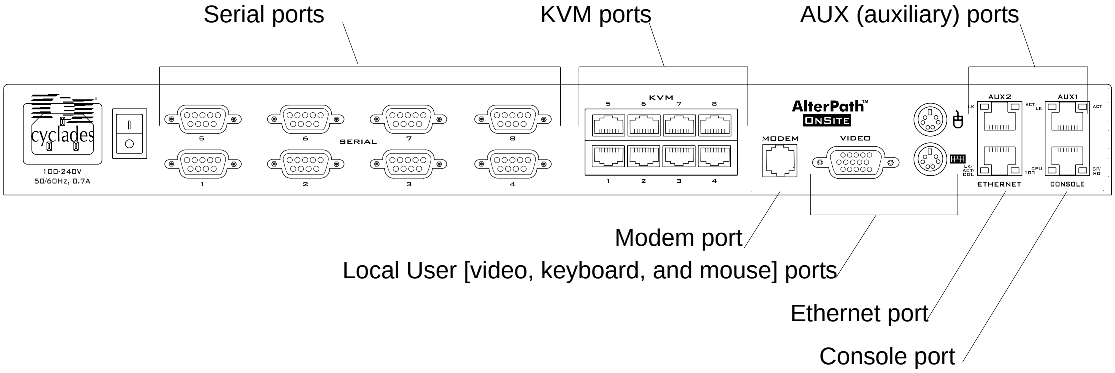


Figure 1-3: OnSite Back with Ports

Power Plug and Serial Ports

The following figure shows the power plug, the power switch, and eight serial ports on the left back of an AlterPath OnSite.

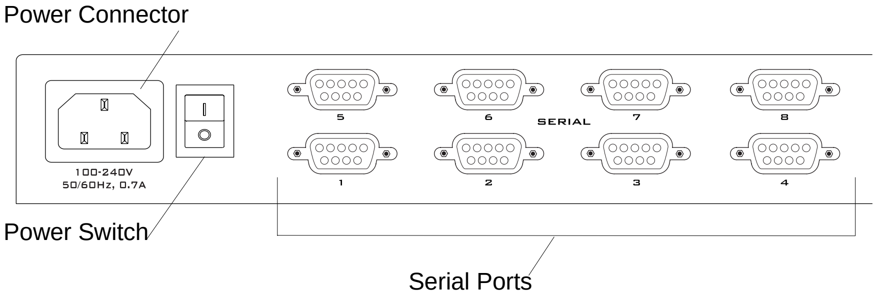


Figure 1-4: Power Connector, Power Switch, and Serial Ports

KVM Ports

In the middle are either four or eight KVM server ports for servers that have keyboard, video, and mouse connections.

The following figure shows eight KVM ports located in the middle of the back of the OnSite. The ports’ RJ-45 connectors accept RJ-45 to RJ-45 CAT5 or greater cables, which plug into AlterPath KVM terminators connected to the server.

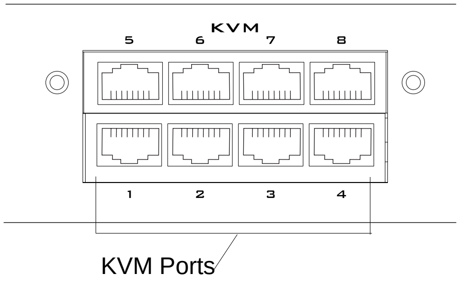


Figure 1-5: KVM Ports

KVM Terminator Usage and Types

An AlterPath KVM 4000 Series Terminator must be connected to the monitor, keyboard, and mouse of a server before the server can be connected to a KVM port. The KVM Terminator converts the server's keyboard, monitor, and mouse signals. After it is connected to the server, the KVM Terminator is connected to a CAT5 or greater cable that has RJ-45 connectors on both ends. The cable, which can be up to 500 feet (152.4 meters) in length, is then connected to a KVM port on the OnSite.

KVM Terminator Models

AlterPath KVM Terminators come in three models shown in the following table:

Table 1-2: AlterPath KVM Series 4000 Terminators, Models, and Part Numbers

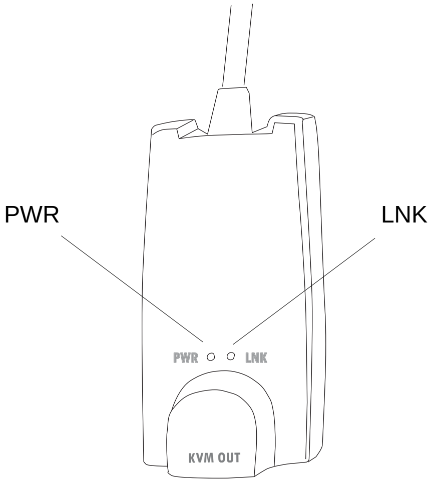
KVM Terminator Connectors	KVM Terminator Model	P/N
VGA (HD-15 male) and PS/2	PS/2	ATP4615
VGA and USB	USB	ATP4635
VGA and Sun Mini-DIN	Sun Mini-DIN	AKP4645

Each AlterPath KVM Terminator is ordered and shipped separately. While ordering an OnSite, the customer orders a KVM Terminator for each server to be connected to the OnSite's KVM ports. For example, when ordering an OnSite with four KVM ports to be connected to two Windows servers with PS/2 connectors and to two Sun servers with VGA ports and USB connectors, the customer would order two PS/2 KVM Terminators and two USB KVM Terminators.

See the "Connecting Servers to KVM Ports" on page 43 for instruction on using the KVM Terminators.

KVM Terminator LEDs

As shown in the following figure, two activity LEDs are located on each KVM terminator near the “KVM Out” end.



- The “PWR” (power) LED blinks green when power is on to the KVM Terminator.
- The “LNK” (link) LED is solid amber when a connection exists between the OnSite and the server. The “LNK” LED blinks amber if the KVM Terminator microcode fails to boot.

Ports on the Right Back

The following figure shows the ports on the right back of the OnSite.

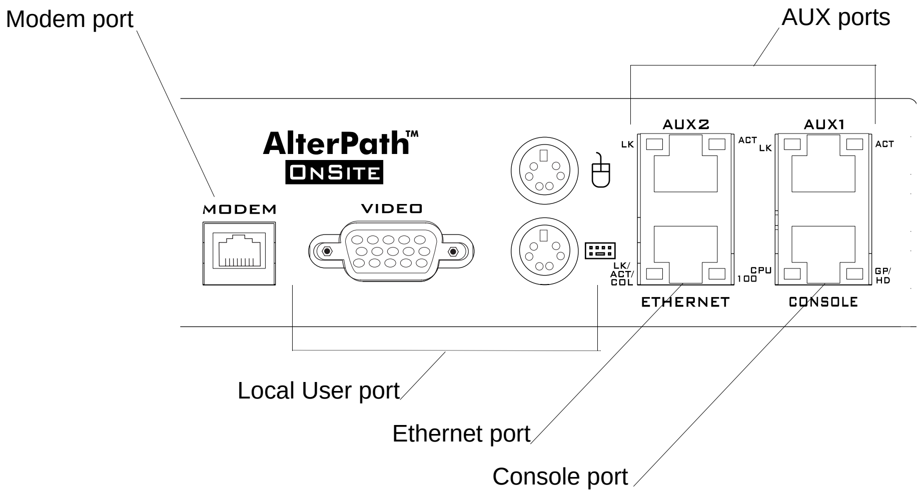


Figure 1-6: Modem, Local User, AUX, Ethernet, and Console Ports

Port LEDs

The following figure shows a close up view of the LEDs on the back of the OnSite. The LEDs monitor the AUX, Ethernet, and console ports as described in Table 1-3.

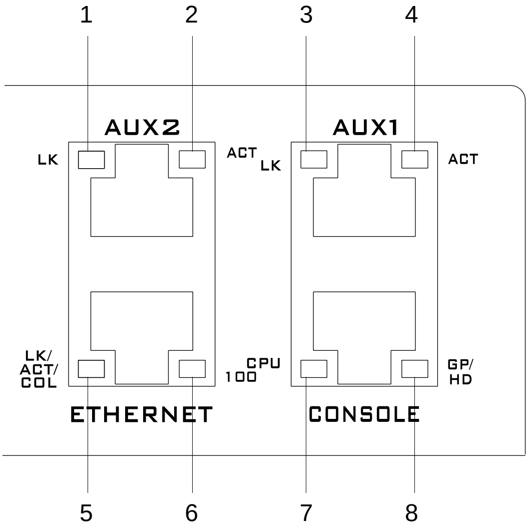


Figure 1-7: LEDs for AUX, Ethernet, and Console Ports

The LED numbers in the tables below correspond to the numbers in the previous figure.

Table 1-3: Port LED Descriptions

Number	Label	Function	Color/Status
1, 3	LK	Monitor RS-232 async port status	• OFF – Indicates the port is not open. • Orange – Lights when DTR (data terminal ready) signal is on (when the port is open).
2, 4	ACT	Monitor RS-232 async activity	• OFF – Indicates no data activity. • Green – Blinks when data is either being received (RX) or transmitted (TX).

Table 1-3: Port LED Descriptions (Continued)

Number	Label	Function	Color/Status
5	LK/ ACT/ COL	Monitor Ethernet line status	• OFF – Indicates either link is not up or cable is not connected. • Green – Lights solid when the link is up and blinks when data activity occurs, with frequency proportional to traffic. • Orange – Blinks when collisions occur
6	100	Monitor Ethernet speed	• Off – Indicates the link is 10baseT or no link is active. • Green – Steady when 100baseT link is active.
7	CPU	Monitor CPU (software operation)	• Off or solid green – During boot and if software crashes. • Green – Blinks when software is operating normally. If software crashes, light stops blinking, and if the Watchdog timer is active, the OnSite reboots.
8	GP/ HD	Monitor compact flash (HD) or other (GP)	Not implemented.

PCMCIA Card Slots on the Front

PCMCIA card slots on the front of the OnSite offer additional remote access and storage options.

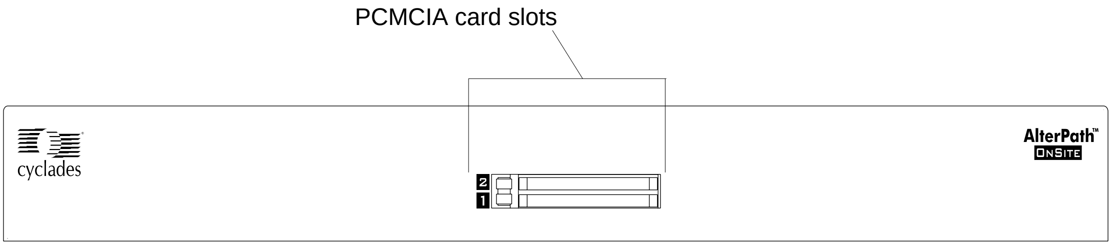


Figure 1-8: PCMCIA Slots on OnSite Front

To see a list of supported PCMCIA cards go to http://www.cyclades.com/products/33/alterpath_onsite. Or go to http://www.cyclades.com > Products > Remote Site Management > AlterPath OnSite, and click the “pc cards list” item on the right side of the page to see the list of supported cards.

The PCMCIA slots support the following types of cards:

- Modem
- ISDN (Integrated Services Digital Network)
- GSM (Global Systems for Mobile communications)/GPRS)
- CDMA
- 10/100 BaseT Ethernet
- Fibre Optic Ethernet
- Compact Flash
- Wireless Ethernet
- IDE hard disk

Consolidated Management Option for Multiple AlterPath Devices

If multiple OnSites or other Cyclades AlterPath devices are installed in multiple remote locations, a Cyclades AlterPath Manager (purchased separately) can be used to manage all the OnSite units together with any other Cyclades products and their connected devices.

OnSite Models and Features

OnSite model numbers and part numbers end with three digits that identify the configuration: 441, 841, 881, and 882. The first digit identifies the number of serial ports, the second digit identifies the number of KVM ports, and the third digit identifies the number of IP modules. For example, ONS841 has 8 serial ports, 4 KVM ports and one IP module.

Connecting to a KVM port over the network (KVM over IP) requires one IP module. Support for a second simultaneous KVM over IP connection requires a second IP module.

The following table shows the model numbers with the numbers of IP modules and numbers and types of server ports available in each model.

Table 1-4: Model Numbers and Configuration Options

Model Number	Part Number	Serial Ports	KVM Ports	IP Modules
ONS441	ATP7441	4	4	1
ONS841	ATP7841	8	4	1
ONS881	ATP7881	8	8	1
ONS882	ATP7882	8	8	2

Customers chose among a number of different AC power cords to suit the electrical requirements of the region where the unit is being installed.

Dial-in Access Types and Options

The following types of devices can be connected to a phone line to enable users to dial into the OnSite:

- The OnSite’s internal modem
- One or more optional external modems connected to an AUX port
- Optional modem PCMCIA card

Optional CDMA and GSM PCMCIA wireless cards can be used for dial-ins also.

All support dial-ins through PPP connections. A PCMCIA modem card can also be accessed for logins from a terminal emulation program.

Once you plug in a modem card and connect it to a dedicated phone line, no configuration is needed to enable dial-in access. However, for callback to work, the OnSite administrator must configure the modem or phone card for callback.

See “Connecting an External Modem to the AUX Port” on page 63 and “Connecting a PCMCIA Modem Card to a Phone Line” on page 64.

IPDU Power Management Options

An AlterPath Power Management (PM) intelligent power distribution unit (IPDU) can be connected to an AUX port on the OnSite 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 ports to manage up to a maximum of 128 outlets.

After an IPDU is connected to the OnSite, 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 OnSite User's and Administrator's Guide)*:

- Configures the AUX port for power management.
- Configures the outlets on connected IPDUs by doing the following tasks:
  - Specifying names to identify devices that are plugged into the outlets
  - Authorizing users to power outlets on and off
- Optionally configuring notifications of over-current states to be sent as alarms to specified users.

When a device is plugged into an IPDU and connected to a serial or KVM port, the user can enter a hot key to bring up a menu or a dialog box to perform power management while connected to the device through the port.

Observe the following rules when plugging servers and other devices into IPDUs.

- Plug servers managed through KVM ports into an IPDU connected to AUX port 1.
- Plug devices managed through serial ports into an IPDU connected to either AUX1 or AUX 2.

The following figure shows an OnSite from the back with IPDUs connected to the AUX1 and AUX2 ports and a second IPDU daisy-chained from the first IPDU.

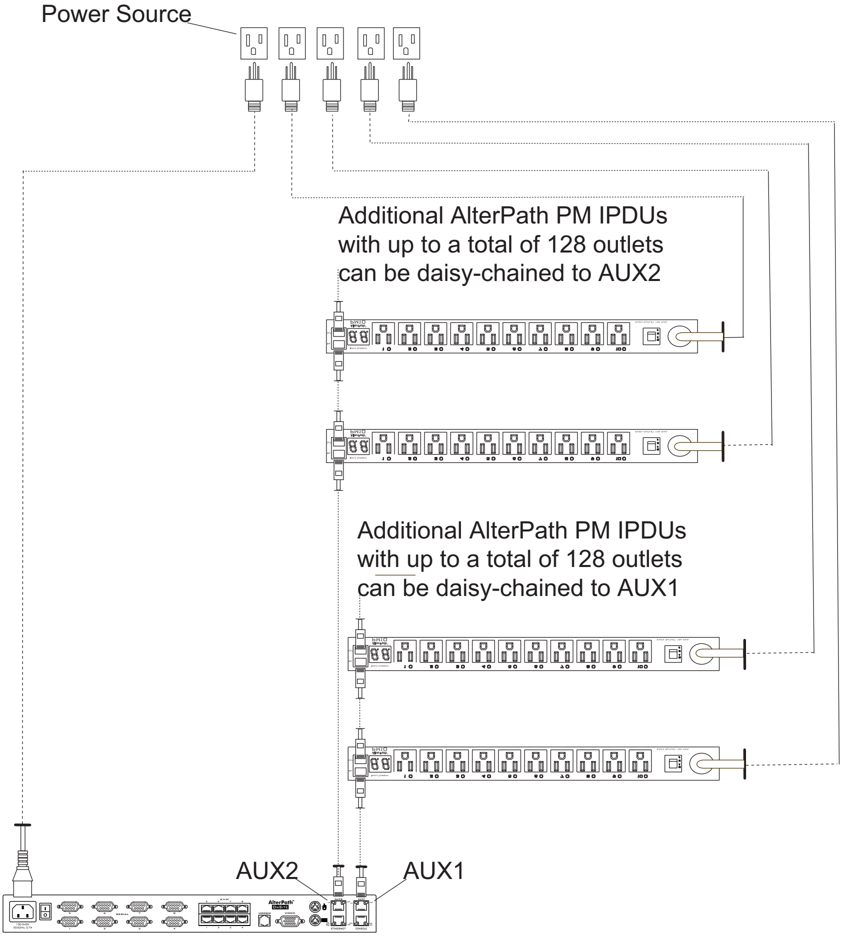

Power Source
Additional AlterPath PM IPDUs
with up to a total of 128 outlets
can be daisy-chained to AUX2
Additional AlterPath PM IPDUs
with up to a total of 128 outlets
can be daisy-chained to AUX1
AUX2
AUX1

Figure 1-9: IPDUs Daisy-Chained to the AUX Ports

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 users to access the command line. The following figure illustrates how local OnSite users can access the command line by logging in through the console port.

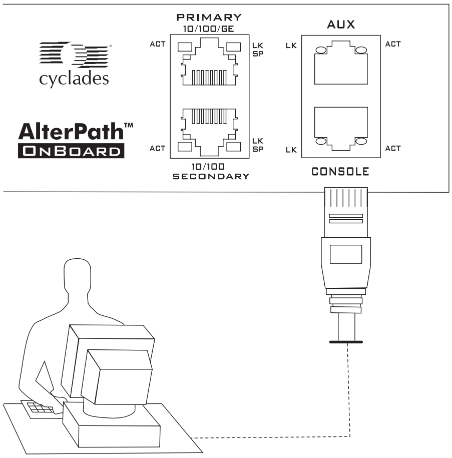


Figure 1-10: User With a Terminal Connected to the Console Port

Authentication Server Options

The administrator chooses a type of authentication to use for accessing the OnSite 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 to be 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 OnSite than for accessing each connected device.
- The OnSite 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 OnSite 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 OnSite.

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

Chapter 2
Installation

This chapter covers the installation topics listed in the following table.

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

Basic Installation

The following figure illustrates some example OnSite connections as they would appear after the basic installation procedures are completed.

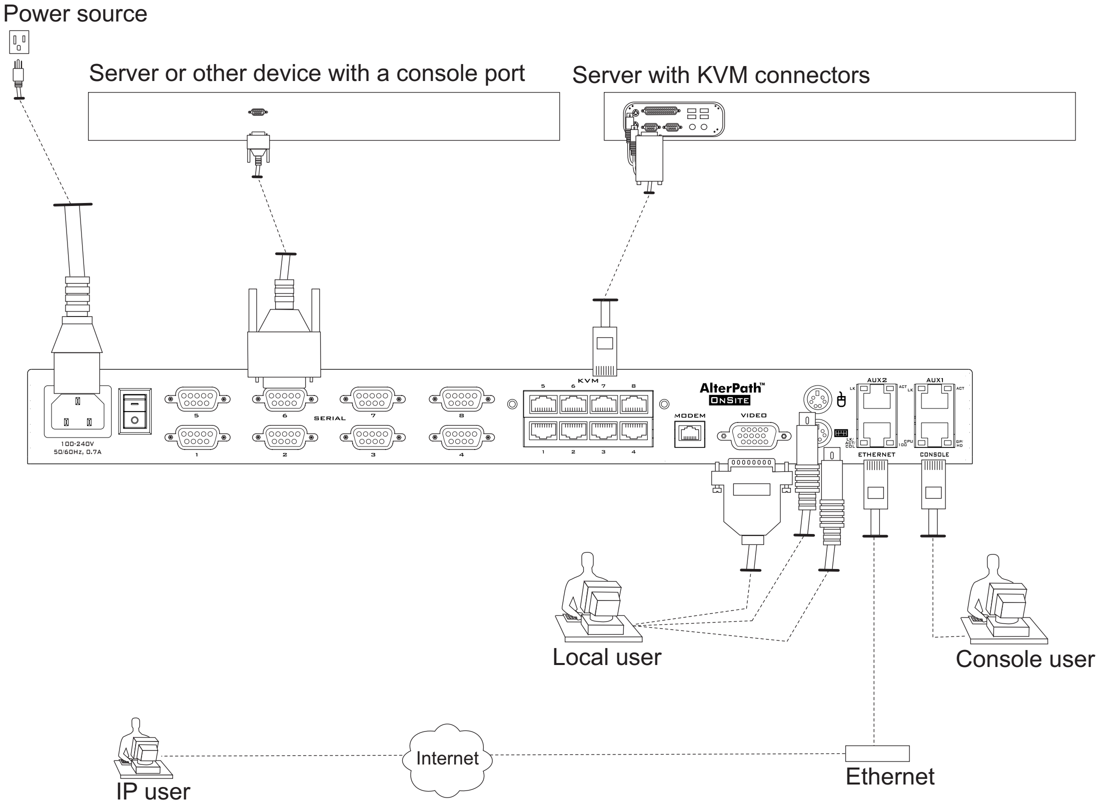


Figure 2-1: Basic Installation Connections Illustrated

The following table lists the basic tasks for installing the AlterPath OnSite 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 21
Rackmount the OnSite.	"Rackmounting the AlterPath OnSite" on page 25
Make a connection to the Ethernet port.	"Making an Ethernet Connection" on page 27
Connect computers and other supported devices to the KVM and serial ports.	"Connecting Devices" on page 27
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:	"Options for Enabling Web Manager Access" on page 47
• Make a connection to the OnSite's console to set a static IP address and other basic network parameters. • Make a connection to the OnSite's Local User port to set a static IP address and other basic network parameters.	• "Making a Local Connection for Configuring Basic Network Parameters" on page 49
Connect the OnSite to a power source and turn the power on.	"Connecting to a Power Source and Turning On the Power" on page 51
Enable access to the Web Manager by assigning a static IP address or configuring a DHCP address.	"Enabling Access to the Web Manager" on page 51
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 58

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

Table 2-2 shows the items shipped with the AlterPath OnSite. The entry 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.

Table 2-2: Shipping Box Contents

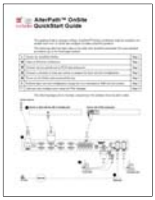
Item	P/N	Description	Purpose
	PAC0266	Documentation CD	PDF copies of this guide and all other Cyclades product documents.
	PAC0342	*AlterPath OnSite QuickStart Guide*	Basic installation guide in printed format. Written for users experienced in installing Cyclades products.

Table 2-2: Shipping Box Contents

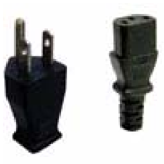
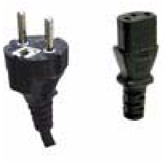
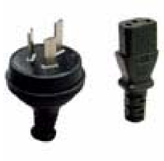
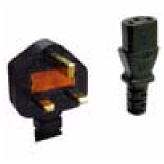
Item	P/N	Description	Purpose
		AC power cable, one of the following.	To connect the OnSite to a power source. The destination county is used to determine which type of cord is shipped based on the country's standard power. The ends of other available cords are shown in the following rows. Talk with a 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.
	CAB0056/ CAB0104	Rectangular blade plug.	UK, Ireland, and other countries.

Table 2-2: Shipping Box Contents

Item	P/N	Description	Purpose
	CAB0278	Flat blades with round grounding pin.	Japan.
	ADB0036	RJ-45 to DB-9 female cross converter adapter	Use for the following purposes: • To connect the console port to a computer that has a DB-9 connector. See “To Connect a Terminal or Computer to the Console Port” on page 49. • To connect a device to one of the OnSite’s serial ports when the device is more than 6 feet away from the OnSite and you want to extend the supplied 6 ft. DB-9 to DB-9 cable (by connecting a CAT5 cable you might have at hand). See “To Extend a DB-9 to DB-9 Cable Connected to a Serial Port” on page 46.

Table 2-2: Shipping Box Contents

Item	P/N	Description	Purpose
	CAB0018	RJ-45 to RJ-45 7ft. CAT5 cable	Use for the following: • To connect a server to a KVM port (with the appropriate AlterPath KVM terminator from Table 1-2 on page 6). See “Connecting Servers to KVM Ports” on page 43. • To connect a device to a serial port (with the supplied ADB0036-000 adapter). See “To Connect a Device’s Console Port to a Serial Port” on page 46. • To connect an Ethernet port to the LAN. See “To Make an Ethernet Connection” on page 27. • To connect a terminal to a console port. See “To Connect a Terminal or Computer to the Console Port” on page 49. • To connect an IPDU or external modem to an AUX ports. See “Connecting One or More IPDUs to the AUX Port” on page 64 and “Connecting an External Modem to the AUX Port” on page 63.
	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, or (less likely) to connect a serial port to a device [with the ADB0036 adapter, and the supplied CAT5, or other standard CAT5 cabling].

Table 2-2: Shipping Box Contents

Item	P/N	Description	Purpose
	CAB00286	DB-9 female to DB-9 female, 6 ft. crossover cable	Use to connect an OnSite serial port to a device with a DB-9 male serial port (the most common serial port connector).
	HAR0220	2 - Mounting brackets with 8 - screws	Use to mount the OnSite to a rack or cabinet. See “To Mount the OnSite in a Rack or Cabinet” on page 26. To mount on a wall, order the brackets under part number: HAR0553.

When ordering the AlterPath OnSite, customers also order one AlterPath KVM Terminator for each server to be connected to one of the KVM ports.The number and types of KVM Terminators is based on the number of KVM ports on the OnSite model that is being shipped and on the types of servers that are to be connected to the KVM ports. For details, see “KVM Terminator Usage and Types” on page 6.

Note: For part ordering information, see “Cyclades Product Guide,” available at: http://www.cyclades.com/common/www/pdf/catalog.en.pdf.

Rackmounting the AlterPath OnSite

You can mount the OnSite in a rack or cabinet or on a wall, or you can place it on a desktop or other flat surface. Two brackets are shipped with the OnSite with screws for attaching the brackets to the OnSite for rack-mounting. Other brackets are available by special order from Cyclades for wall mounting.

Caution: Observe all safety precautions described in Appendix B, “Safety Information,” especially making sure to load the rack from the bottom up.

Before you start, make sure you have the following:

- The mounting brackets and the eight Phillips screws
- A Phillips screwdriver
- Appropriate nuts and bolts for attaching the brackets to the rack

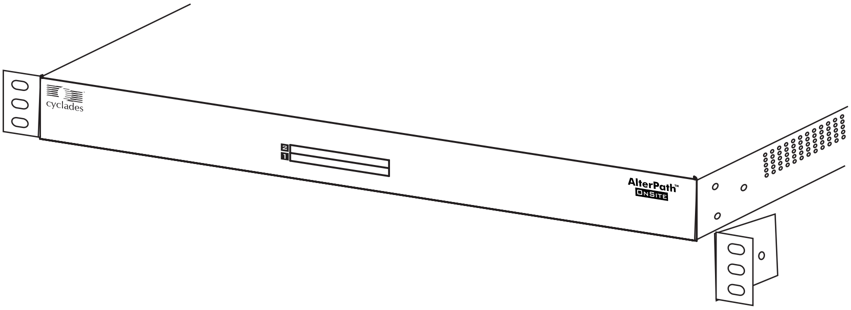
Decide whether to mount the OnSite on the front or back and locate the appropriate sets of holes on the OnSite.

▼ To Mount the OnSite in a Rack or Cabinet

1. Connect the two brackets to the OnSite, connecting a bracket to each side.

   For each bracket, insert three screws through the holes on the bracket into the appropriate holes at either the front or back of the OnSite.

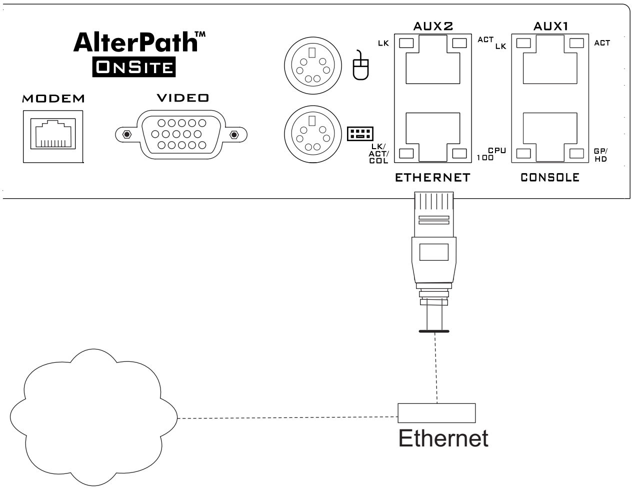
   The following figure shows the angle of a bracket being installed so that the OnSite can be mounted on the front posts of a rack.



2. Use a Phillips screwdriver to tighten the screws.
3. Use screws or nuts and bolts as appropriate to mount the OnSite on the wall, on a rack, or in a cabinet.

Making an Ethernet Connection

Use the RJ-45 to RJ-45 Ethernet CAT5 cable shipped with the OnSite or an off-the-shelf equivalent (CAT5 or greater) to connect the Ethernet port to an Ethernet switch, router, or local area network (LAN) port. The following figure shows connecting an RJ-45 connector to the Ethernet port on the OnSite.



▼ *To Make an Ethernet Connection*

1. Connect one end of a RJ-45 to RJ-45 CAT5 or greater Ethernet cable to an Ethernet switch, router, or LAN port.
2. Connect the other end to the Ethernet port on the OnSite.

Connecting Devices

The following table lists the sections related to connecting servers to the KVM ports and connecting serially-managed devices to the serial ports:

Preparing to Connect Devices to the OnSite	Page 28
Mouse Settings Requirements for KVM Port Access	Page 34
ActiveX Requirements for KVM Port Access	Page 44
Java Plug-in Requirements for Serial Port Access	Page 46

Connecting Servers to KVM Ports	Page 43
Connecting Devices to Serial Ports	Page 46

Preparing to Connect Devices to the OnSite

The following prerequisites must be completed before connected devices can communicate with the OnSite.

1. Make sure all configuration is complete on servers and other devices to be connected.

   Work with the administrators of the devices to ensure all the following prerequisites are complete:

   - All devices are installed and fully configured.
   - User accounts exist on each device for every user who needs access to the device, and you have the usernames and passwords to give to users who need to access the device.
   - You have the administrator's password to give to users who need to administer the device.

2. When the OnSite or connected devices are going 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) that is needed to configure the authentication server on the OnSite.

Note: After the OnSite is installed, make sure to configure the desired authentication method for each device as described in the *AlterPath OnSite Administrator's and User's Guide*."

3. On all servers to be connected to KVM server ports, make sure the mouse settings are configured to support synchronization between the remote user's mouse and the local server.

   A remote user's mouse cannot track over the KVM connection unless the settings are correct on the server. Work with the administrator of the servers to ensure that the settings are correct, as described in “Mouse Settings Requirements for KVM Port Access” on page 29.

4. In the browser of each user who needs to access a server through a KVM port., make sure that the ActiveX plug-in is enabled.

   See “ActiveX Requirements for KVM Port Access” on page 34.

5. In the browser of each user who needs to access a device through a serial port, make sure that the Java plug-in is installed on the computer and registered with the browser.

   Access to serial ports is through the Java applet viewing window, which relies on Java 2 Runtime Environment (J2RE) software being installed on the computer and the Java plug-in enabled in the browser.

   See “Java Plug-in Requirements for Serial Port Access” on page 42.

Mouse Settings Requirements for KVM Port Access

When a server connected to a KVM port is being accessed through the Web Manager, make sure that the prerequisite configuration is complete on the server to ensure that the remote user’s mouse tracks properly. The following table lists the different procedures for the supported server types.

Table 2-3: Tasks for Synchronizing Mouse Tracking on Servers Connected to KVM Ports

To Modify Mouse Settings on Windows XP/Windows 2003 Servers	Page 30
To Modify Mouse Settings on Windows 2000/ME Servers	Page 31
To Modify Mouse Settings on Windows 95/98/NT Servers	Page 32
To Modify Mouse Settings on Linux Servers	Page 33

Note: Checking and possible resetting of the mouse parameters must be done after every server reboot.

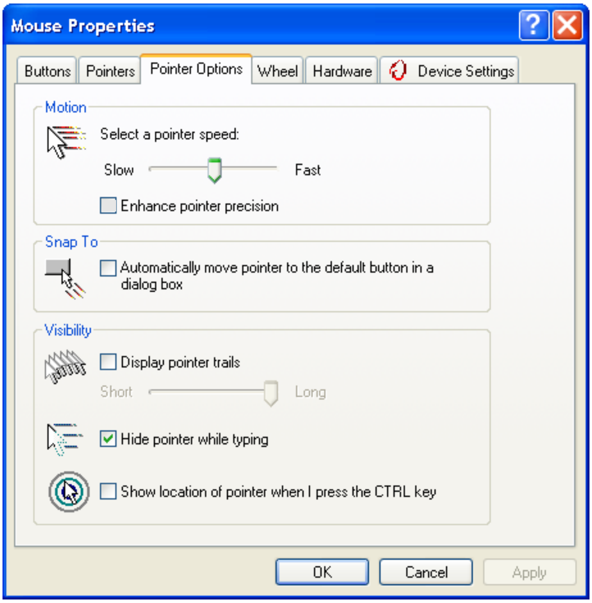
▼ *To Modify Mouse Settings on Windows XP/ Windows 2003 Servers*

Make sure that this procedure is performed on any server to be connected to one of the KVM ports, when the server is running Windows XP or Windows 2003. Refer to “Mouse Settings Requirements for KVM Port Access” for background information, if needed.

Note: Perform this procedure to synchronize mouse settings after every reboot.

1. As administrator, on the Start Menu, go to: Control Panel >Mouse> Pointer Options.
2. To disable “Enhance pointer precision,” click the checkbox to uncheck it.
3. To set the motion speed to medium, move the slider to the middle of the “Select a pointer speed” scale.

   The Effects settings should look like those shown in the figure below.


Mouse Properties

Motion

Select a pointer speed:

Slow — Fast

□ Enhance pointer precision

Snap To

□ Automatically move pointer to the default button in a dialog box

Visibility

□ Display pointer trails

Short — Long

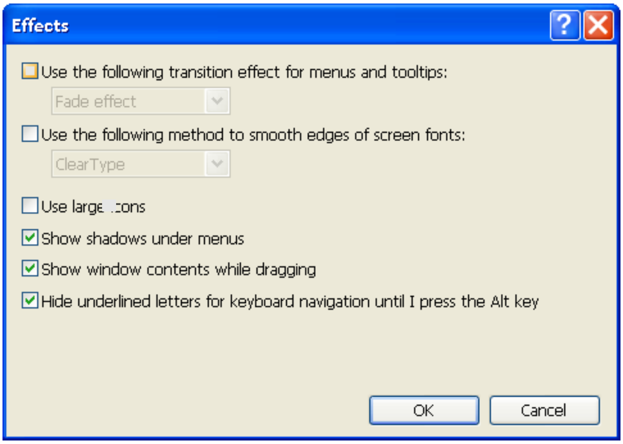
☑ Hide pointer while typing

□ Show location of pointer when I press the CTRL key

4. Click OK.
5. Go to: Control Panel>Display >Appearance>Effects.

6. Click the checkbox next to “Use the following transition effect for menus and tooltips” to uncheck it.

   The Mouse Properties settings should look like those shown in the figure below.



Effects

□ Use the following transition effect for menus and tooltips:

Fade effect

□ Use the following method to smooth edges of screen fonts:

ClearType

□ Use large icons

☑ Show shadows under menus

☑ Show window contents while dragging

☑ Hide underlined letters for keyboard navigation until I press the Alt key

7. Click OK.
8. Click OK in the appearance dialog box.
9. Click the X at the upper right of the window to close the “Control Panel” dialog box.

▼ *To Modify Mouse Settings on Windows 2000/ME Servers*

Make sure that this procedure is performed on any server connected to one of the KVM ports, when the server is running Windows 2000 or Windows ME.

1. As administrator, on the Start menu, go to: Settings>Control Panel>Mouse>Pointer Options.
2. To set the mouse pointer acceleration to none, do the following:

   a. Click the “Advanced” button.

      The “Advanced Setting Pointer Speed” dialog box appears.

   b. On Windows ME, uncheck the “Pointer acceleration” check box.

   c. On Windows 2000, uncheck the “Enable pointer acceleration” check box.

   d. Click OK.

3. Set the motion speed to medium by moving the slider to the middle of the “Adjust how fast the pointer moves” scale.

4. Click OK.

5. To disable transition effects do the following:

   a. Go to: Control Panel>Display>Effects.

   b. Uncheck Use transition effects for menus and tooltips.

   c. Click OK.

6. Click the X at the upper right of the window to close the “Control Panel” dialog box.

▼ *To Modify Mouse Settings on Windows 95/98/ NT Servers*

Make sure that this procedure is performed on any server connected to one of the KVM ports, when the server is running the Windows 95 or Windows 98 operating system.

Note: Perform this procedure to synchronize mouse settings after every reboot.

---

1. As administrator, on the Start menu, go to: Setings>Control Panel>Mouse>Motion.

2. Set the motion speed by moving the slider to the lowest setting on the “Pointer Speed” scale.

3. Go to: Settings>Control Panel >Display >Effects>Advanced Settings for Pointer Speed.

4. Disable window, menu, and list animation by unchecking “Animate windows, menus, and lists.”

5. Click OK.

6. Click the X at the upper right of the window to close the dialog box.

▼ *To Modify Mouse Settings on Linux Servers*

Make sure that this procedure is performed on any server connected to one of the KVM ports, when the server is running the Linux operating system.

Note: Perform this procedure to synchronize mouse settings after every reboot.

This procedure assumes that you have the login name and password for an account configured with the following types of access:

- Access on the OnSite to the port where the computer is connected
- Access as root on the connected computer running Linux without a window system

1. Log into the Cyclades Web Manager with the username and password of an account that has been configured to access the port where the computer is connected.
2. Go to Expert>Access>Connect to Server.
3. From the pull-down menu select the port number or alias for the computer, and click the Connect button.
4. If port authentication is configured, log into the server as root.

The root prompt appears.

```
#
```

5. Disable the mouse pointer acceleration and threshold settings by entering the **`xset m 0`** command:

```
# xset m 0
```

6. Exit the AlterPath Viewer.

ActiveX Requirements for KVM Port Access

The AlterPath Viewer relies on the ActiveX plug-in. Different browsers vary in whether or not ActiveX is enabled, as described in the following bulleted list:

- With some supported Netscape versions, the ActiveX plug-in is shipped by default, but the plug-in is not enabled.
- In some versions of Internet Explorer (IE) browsers, the ActiveX plug-in is shipped by default, but the plug-in is not enabled.
- For Mozilla, the ActiveX plug-in is not shipped, so the user needs to download and install the appropriate ActiveX plug-in.

The user needs to make sure that the ActiveX plug-in is enabled in the browser before it can be used to access a server through a KVM port. The procedures for enabling ActiveX are listed in the following table.

Table 2-4: Tasks for Enabling ActiveX for AlterPath Viewer Support

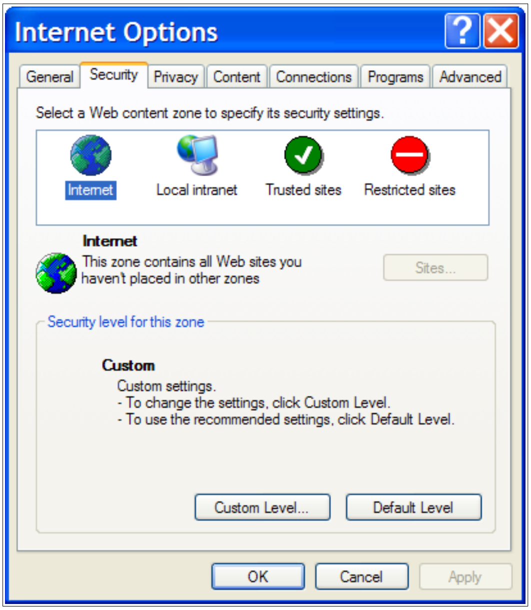
To Enable ActiveX in Internet Explorer	Page 34
To Enable ActiveX in Netscape 7.x	Page 36
To Enable ActiveX on Netscape 8.x	Page 37
To Download and Install the ActiveX Plug-in for Mozilla or Firefox	Page 41

▼ To Enable ActiveX in Internet Explorer

The user of a remote computer performs this procedure to enable ActiveX in Internet Explorer, to allow the browser to access KVM ports through the OnSite.

1. In Internet Explorer, go to Tools>Internet Options>Security.

   The Security dialog box appears.



Select a Web content zone to specify its security settings.

Internet

This zone contains all Web sites you haven't placed in other zones

Security level for this zone

Custom

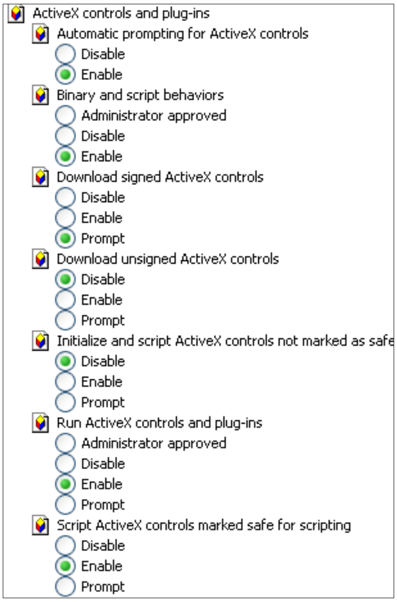
Custom settings.
- To change the settings, click Custom Level.
- To use the recommended settings, click Default Level.

2. Click the “Custom Level” button.

   The “Security Settings” screen appears.

3. On the Security Settings screen, scroll to “Download signed ActiveX controls.”

4. Select the “Enable” and “Disable” radio buttons as shown in the following figure, and click OK.



- ActiveX controls and plug-ins
  - Automatic prompting for ActiveX controls
    - ○ Disable
    - ● Enable
  - Binary and script behaviors
    - ○ Administrator approved
    - ○ Disable
    - ● Enable
  - Download signed ActiveX controls
    - ○ Disable
    - ○ Enable
    - ● Prompt
  - Download unsigned ActiveX controls
    - ● Disable
    - ○ Enable
    - ○ Prompt
  - Initialize and script ActiveX controls not marked as safe
    - ● Disable
    - ○ Enable
    - ○ Prompt
  - Run ActiveX controls and plug-ins
    - ○ Administrator approved
    - ○ Disable
    - ● Enable
    - ○ Prompt
  - Script ActiveX controls marked safe for scripting
    - ○ Disable
    - ● Enable
    - ○ Prompt

▼ *To Enable ActiveX in Netscape 7.x*

The user of a remote computer performs this procedure to enable ActiveX in Netscape 7.x, to allow the browser to access KVM ports through the OnSite. The example shows the path to the Netscape directory in a Windows computer.

1. Open the `activex.js` file for editing:

```
C:\Program Files\Netscape\defaults\pref\activex.js
```

2. Add the following line or modify the line if it already exists, so that it appears as shown in the following screen example.

```
pref("security.classID.allowByDefault", true);
```

3. Save and quit the file.

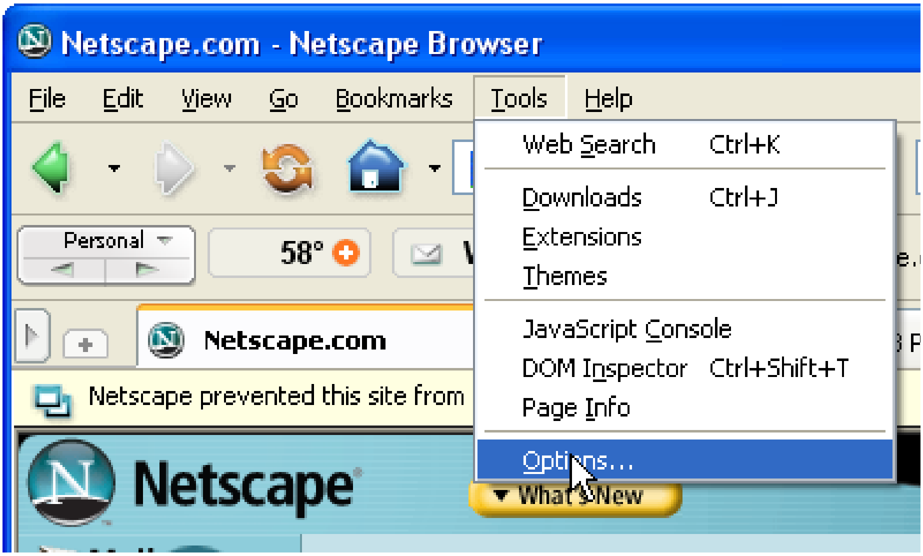
4. Restart Netscape 7.x.

▼ *To Enable ActiveX on Netscape 8.x*

The user of a remote computer performs this procedure to enable ActiveX in Netscape 8.x, to allow the browser to access KVM ports through the OnSite. The example shows the path to the Netscape directory in a Windows computer.

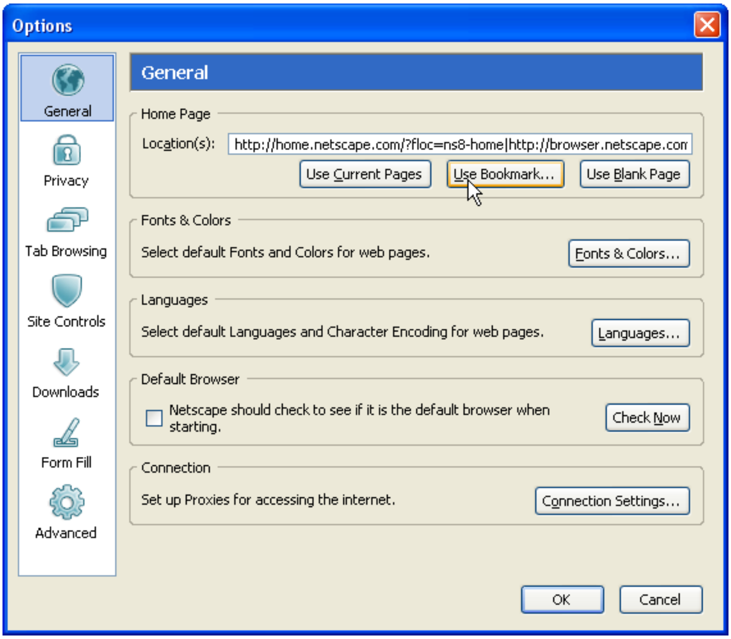
1. Open a Netscape 8.x Browser.

2. On the pull-down menu bar, go to the Tools > Options.


Netscape.com - Netscape Browser
File Edit View Go Bookmarks Tools Help
Web Search Ctrl+K
Downloads Ctrl+J
Extensions
Themes
JavaScript Console
DOM Inspector Ctrl+Shift+T
Page Info
Options...
Personal
58°
Netscape.com
Netscape prevented this site from
Netscape
What's New

3. Click on “Options”

An “Options” window appears.



Location(s): http://home.netscape.com/?floc=ns8-home|http://browser.netscape.con

Select default Fonts and Colors for web pages.

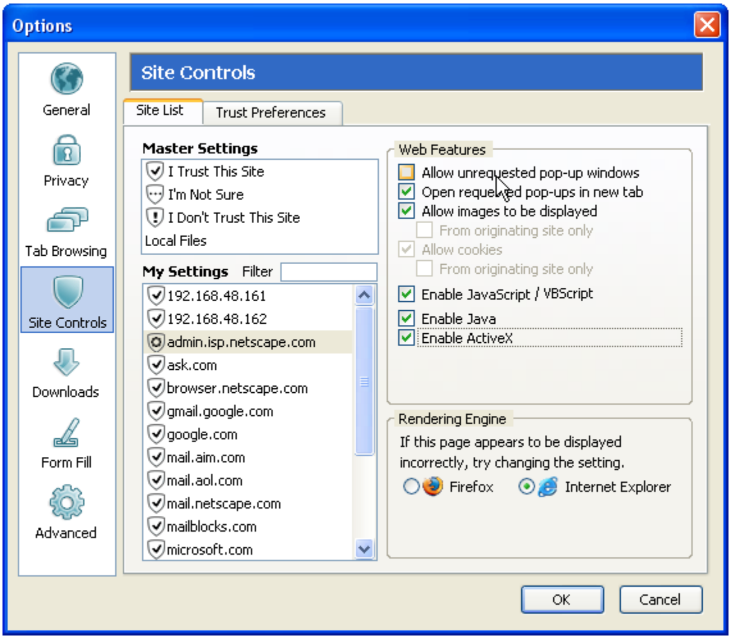
Select default Languages and Character Encoding for web pages.

□ Netscape should check to see if it is the default browser when starting.

Set up Proxies for accessing the internet.

4. Click on “Site Controls” in the left column of the window.

The window that appears has the button to enable ActiveX.



Options

Site Controls

Master Settings

- I Trust This Site
- I'm Not Sure
- I Don't Trust This Site
- Local Files

My Settings Filter

- 192.168.48.161
- 192.168.48.162
- admin.isp.netscape.com
- ask.com
- browser.netscape.com
- gmail.google.com
- google.com
- mail.aim.com
- mail.aol.com
- mail.netscape.com
- mailblocks.com
- microsoft.com

Web Features

- □ Allow unrequested pop-up windows
- ☑ Open requested pop-ups in new tab
- ☑ Allow images to be displayed
- □ From originating site only
- ☑ Allow cookies
- □ From originating site only
- ☑ Enable JavaScript / VBScript
- ☑ Enable Java
- ☑ Enable ActiveX

Rendering Engine

If this page appears to be displayed incorrectly, try changing the setting.

○ Firefox ● Internet Explorer

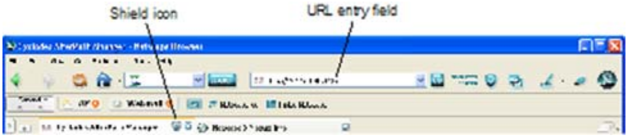
5. Select “Internet Explorer” in the “Rendering Engine” box in the lower right of the window.

6. Select “Enable ActiveX” in the “Web Features” box.

7. Click the “OK” button.

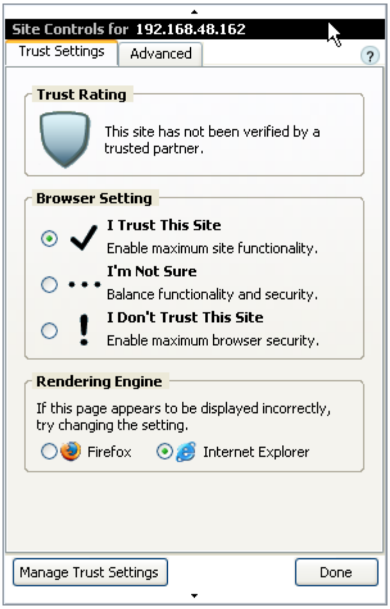
8. Enter the IP address of the OnSite in the URL entry field of your Netscape browser.

9. Notice the shield icon shown in the following figure.



10. Click on the Shield Icon.

A “Trust Settings” dialog box appears.



Trust Rating

This site has not been verified by a trusted partner.

Browser Setting

● I Trust This Site
Enable maximum site functionality.

○ I'm Not Sure
Balance functionality and security.

○ I Don't Trust This Site
Enable maximum browser security.

Rendering Engine

If this page appears to be displayed incorrectly, try changing the setting.

○ Firefox ● Internet Explorer

11. Click on the “I Trust This Site” button.

ActiveX is enabled, and the computer’s IP is marked as a trusted site.

▼ *To Download and Install the ActiveX Plug-in for Mozilla or Firefox*

The user of a remote computer performs this procedure to enable ActiveX for Mozilla or Firefox.

You can download Mozilla and Firefox from http://www.mozilla.org/products.

1. Open the Mozilla or Firefox browser.

2. Go to http://www.iol.ie/~locka/mozilla/plugin.htm.

3. Click “Download the plug-in” in the left navbar.

4. Click the “Click here” link next to the product version.

A prompt appears asking you to give permission to install the plug-in.

5. Click “Install.”

A dialog displays a “Successful installation” notice.

6. Close and restart the browser.

Java Plug-in Requirements for Serial Port Access

The Java plug-in must be installed on the computer and registered with a browser for a user to be able to access a serial port using the Java applet viewing window. Installing Java 2 Runtime Environment (J2RE) software, Standard Edition, Version 1.4.2 automatically installs the needed Java plug-in.

Note: The Java Runtime Environment is also called Java 2 Platform, Standard Edition (J2SE) at the java.sun.com website.

The following table provides links to the related procedures.

To Check Browsers for Java Plug-in Support	Page 42
To Install JRE2 Software and Register the Java Plug-in	Page 43

▼ To Check Browsers for Java Plug-in Support

1. Open the browser.
2. Go to the following URL:

```
http://java.com/en/download/installed.jsp
```

3. Click the “Verify Installation” button.
4. The verification program checks that the latest JRE version is installed on the computer and that the Java Plug-in is registered in the current browser.
5. Go to “To Install JRE2 Software and Register the Java Plug-in” on page 43 if the following occur.

   - If the verification indicates that JRE is not installed.

   OR

   - The computer and browser do not have the latest version and you want to use the latest version.

▼ *To Install JRE2 Software and Register the Java Plug-in*

1. Make sure the Java 2 Runtime Environment (JRE 2) software, version 1.4.2 or greater is installed on the computer.

   If needed, download the JRE 2 software from the following URL

```
http://java.sun.com/javase/downloads/index.html
```

2. Enable the Java plug-in.

   See the instructions at the java.com website. For example, the following URL has instructions about enabling the Java plugin in Internet Explorer, Netscape, Mozilla, and Firefox after installation of JRE 2 version 1.5.

```
http://java.com/en/download/help/5000020500.xml
```

3. Verify that the browser is successfully registered with the browser by performing this procedure: “To Check Browsers for Java Plug-in Support” on page 42.

Connecting Servers to KVM Ports

Connect servers to KVM ports after completing “Preparing to Connect Devices to the OnSite” on page 28.

You need to connect a KVM Terminator to every server that is to be connected to a KVM port. See “KVM Terminator Usage and Types” on page 6 for more details about the KVM Terminators, which are ordered and shipped with the AlterPath OnSite.

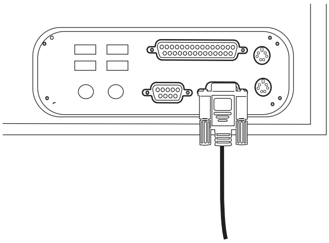
Between the KVM terminator’s RJ-45 connector and the OnSite’s KVM port, you can use up to 500 ft. of RJ-45 to RJ-45 CAT5 or greater straight-through cable.

Note: KVM port connections rely on the cable having all four pairs wired. If you are connecting a KVM port to a server through a patch panel, make sure that all cables in the path are CAT5 or greater and that the patch panel has all four pairs wired.

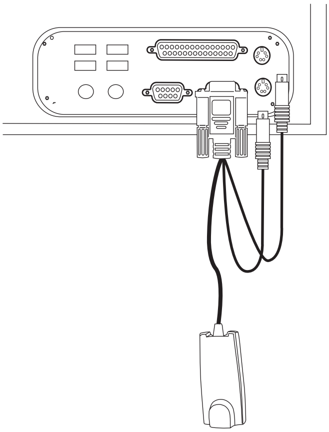
▼ *To Connect a Server to a KVM Port*

1. Select the appropriate KVM Terminator for the type of server being connected to the KVM port.

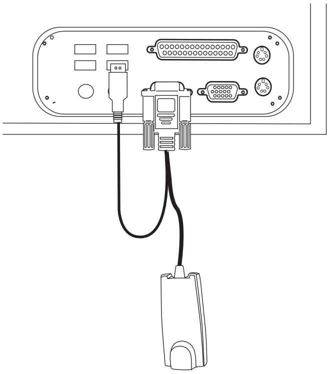
2. Connect the KVM Terminator's VGA (HD-15 male) connector to the server's VGA (monitor) port, tightening both screws firmly but not over-tightening.



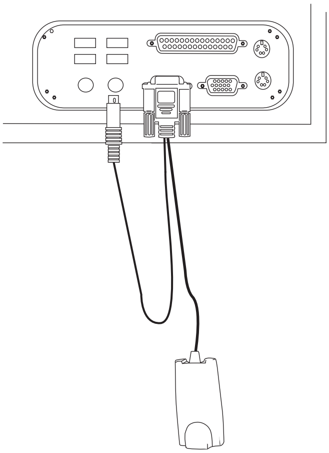
3. To complete the connection of a PS/2 KVM Terminator to a Windows server, connect the KVM Terminator's green connector to the green mouse port and the purple connector to the purple keyboard port on the PC.



4. To complete the connection of a USB KVM Terminator, plug the USB connector from the KVM Terminator to the computer's USB port.



5. To complete the connection of a Sun Mini-DIN KVM Terminator, plug the Sun Mini-DIN connector from the KVM Terminator into the Sun Mini-DIN port.



6. Insert one end of an RJ-45 to RJ-45 CAT5 cable up to 500 feet long into the KVM Out end of the terminator.

7. Connect the RJ-45 connector on other end of the cable to a KVM port on the OnSite.

8. Repeat Step 1 through Step 7 for all servers to be connected to the KVM ports.

Connecting Devices to Serial Ports

Connect servers to serial ports after completing “Preparing to Connect Devices to the OnSite” on page 28.

▼ To Connect a Device’s Console Port to a Serial Port

Perform the following steps after completing “Preparing to Connect Devices to the OnSite” on page 28. This procedure assumes you have the six ft. DB-9 to DB-9 crossover cable shipped with the OnSite or an off-the-shelf equivalent. If you want to extend the supplied cable or use regular CAT5 or greater cable with RJ-45 connectors, see the following procedures:

To Extend a DB-9 to DB-9 Cable Connected to a Serial Port	Page 46
To Connect a Dumb Terminal to a Serial Port	Page 47

1. Connect one end of a DB-9 to DB-9 crossover cable to a serial port on the OnSite.
2. Connect the other end of the cable to the console port on the device.

▼ To Extend a DB-9 to DB-9 Cable Connected to a Serial Port

Perform this procedure if a device that you want to connect to a serial port is further than six feet away and therefore out of the reach of the standard DB-9 to DB-9 seven ft. crossover cable shipped with the OnSite, or if you want to extend an equivalent cable. Alternately, you can purchase a DB-9 to DB-9 cable that’s long enough for your purposes, up to a maximum of 50 feet.

For the list of items shipped with the OnSite, see “Shipping Box Contents” on page 21.

This procedure assumes you have the following items:

- The supplied six ft. DB-9 to DB-9 crossover cable or an off-the-shelf equivalent
- The supplied RJ-45 to DB-9 female crossover adapter
- RJ-45 to RJ-45 CAT5 cable long enough to reach the device
- A non-crossover adapter (DB-9 or DB-25) compatible with the console port on the device

1. Mount the OnSite.

2. Connect one end of the DB-9 to DB-9 crossover cable to the desired serial port.
3. Connect the RJ-45 to DB-9 female crossover adapter to the other end of the cable.

▼ *To Connect a Dumb Terminal to a Serial Port*

Perform the following steps to connect a dumb terminal to a serial port on the OnSite. You need a crossover cable with a DB-9 connector on one end and a connector on the other end that matches the type of connector on the terminal (usually DB-9 or DB-25).

1. Connect the DB-9 end of the crossover cable to one of the OnSite's serial ports
2. Connect the other end of the cable to the dumb terminal.
3. Set up the terminal according to the terminal's manual.
4. Note the following terminal settings that you need to use when configuring the serial port on the OnSite.
    - Baud Rate: ____________________
    - Data Length: ____________________
    - Parity: ____________________
    - Stop Bits: ____________________
    - Flow Control: ____________________
    - ANSI emulation: ____________________
    - Terminal type: ____________________

Options for Enabling Web Manager Access

An administrator who knows the password for an administrative user account and who has network access to the OnSite needs to enter the OnSite'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.

Before the administrator can bring up the Web Manager to finish configuration, one of the tasks in the following table must be performed to either set a static IP address or set up a DHCP server.

Table 2-5: Options for Enabling Web Manager Access

Method	Considerations	Where Described
Make a local connection to configure a static IP address: • Connect a terminal to the console port and use the `wiz` command to configure a static IP address. OR • Connect a monitor, keyboard, and mouse to the Local User ports and use the OSD to configure a static IP address.	You must be at the same location as the OnSite to make the local connection.	• "Making a Local Connection for Configuring Basic Network Parameters" on page 49
Use a DHCP-assigned address.	DHCP is enabled by default. It relies on a DHCP server that must be available to the OnSite.	"To Use a Dynamic IP Address to Access the Web Manager" on page 56
Use the default OnSite 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 OnSite to be able to use the default IP address in launching the Web Manager.	"To Use the Default IP Address to Access the Web Manager" on page 56

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

- Hostname: ____
- OnSite’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: _________________________________

Making a Local Connection for Configuring Basic Network Parameters

You can make a local connection to enable configuration of a static IP address in one of the two following ways.

- Connect a terminal to the console port as described in “To Connect a Terminal or Computer to the Console Port” on page 49.

OR

- Connect a monitor, keyboard, and mouse to the Local User ports as described in “To Connect to the Local User Management Port” on page 50.

▼ *To Connect a Terminal or Computer to the Console Port*

Perform the following steps to connect a terminal or a computer to the console port of the OnSite. 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.

An RJ-45 to DB-9 6 ft. crossover cable is shipped with the OnSite for the connection. Be sure that whatever cable you use is a crossover cable. This procedure assumes you have the RJ-45 to DB-9 6 ft. CAT5 cable shipped with the OnSite 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.

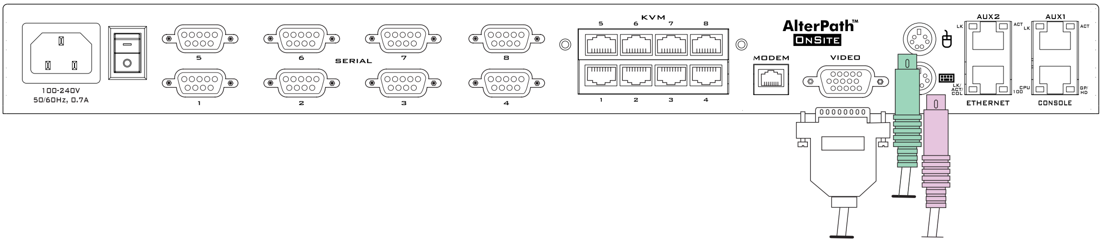
1. If connecting to a computer or terminal with a DB-9 male port, perform these steps.
   a. Connect the RJ-45 end of the cable to the OnSite’s console port.
   b. Connect the DB-9 female end of the cable to the DB-9 connection on the terminal or computer.
2. If connecting to a computer or terminal with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

▼ *To Connect to the Local User Management Port*

Connect the cables from a keyboard, monitor, and mouse into the keyboard, video, and mouse ports on the right back of the OnSite.

- Plug cables from a monitor, keyboard, and mouse to the keyboard, video and mouse ports on the OnSite.

  The following figure illustrates the keyboard, video and mouse cables being connected to the OnSite.



Connecting to a Power Source and Turning On the Power

Do the following procedures in the order shown to avoid problems with components on connected devices that may not be hot-pluggable.

▼ *To Power On the OnSite*

1. Make sure the OnSite’s power switch is off.
2. Plug the power cord into the OnSite and plug the other end into an appropriate grounded AC power source.
3. Turn the OnSite’s power switch on.

▼ *To Power On Connected Devices*

- Turn on the power switches of the connected computers and devices.

Enabling Access to the Web Manager

Perform one of the procedures in this section to enable a remote administrator to finish configuration using the Web Manager. See Table 2-5, “Options for Enabling Web Manager Access,” on page 48 for details about each method.

Configuring Basic Networking Using the wiz Command

This procedure requires a terminal or a computer that has a terminal emulation program to be physically connected to the console port of the OnSite. See “To Connect a Terminal or Computer to the Console Port” on page 49.

▼ *To Configure Basic Network Parameters Using the wiz Command*

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

Table 2-6: 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. From the terminal or terminal emulation program, log into the console port as root.

```
OnSite login: root
Password: cyclades
[root@OnSite /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@OnSite /root]# passwd
```

4. Enter a new password when prompted.

```
New password: new_password

Re-enter new password: new_password

Password changed
```

1. Launch the Configuration Wizard by entering the `wiz` command.

```
[root@OnSite /]# wiz
```

2. At the prompt, enter **`n`** to change the defaults.

```
Set to defaults (y/n)[n]: n
```

3. Click “Enter” to accept default hostname, otherwise enter your own hostname.

   The following example uses `boston_branch_onsite` as the hostname.

```
Hostname [onsite]: boston_branch_onsite
```

4. Click “Enter” to disable DHCP.

```
Do you want to use DHCP to automatically assign an IP for your system?  (y/n)[n]: n
```

5. Enter a public IP address to assign to the OnSite.

```
System IP[192.168.160.10]: public_IP_address
```

6. Enter the domain name.

```
Domain name[cyclades.com]: domainname
```

7. Enter the IP address of the DNS (domain name) server.

```
Primary DNS Server[192.168.44.21] : DNS_server_IP_address
```

8. Enter the IP address for the gateway.

```
Gateway IP[eth0] : gateway_IP_address
```

9. Enter the netmask for the subnetwork.

```
Network Mask[#] : netmask
```

10. Review the values of all the network configuration parameters, as shown in the following screen example. The values shown are for example only.

```
Current configuration:

Hostname : onsite
DHCP : disabled
System IP : 192.168.45.32
Domain name : cyclades.com
drwxr-xr-x    1 root
Primary DNS Server : 192.168.44.21
Gateway IP : 198.168.44.1
Network Mask : 255.255.252.0
Are all these parameters correct? (y/n) [n] :
```

11. Enter **y**.

    The following prompt appears.

```
Are all the parameters correct? (y/n)[n]: y
```

12. Enter **y** to save the changes.

```
Do you want to save your configuration to Flash? (y/n)[n]: y
```

13. To confirm the configuration, enter the `ifconfig` command.

    The new network parameters display.

14. Log out from the terminal session.

15. In a HyperTerminal application on a Windows PC, go to “File>Exit”.Log out.

16. Go to “Selecting a Security Profile, Adding Users and Configuring Devices Using the Web Manager” on page 58.

Configuring Basic Networking Using the OSD

Using the OSD requires a hardware connection already made between the OnSite’s Local User ports and a local monitor, keyboard, and mouse, as described under “To Connect to the Local User Management Port” on page 50. After the OnSite and the monitor are powered on, the OSD login screen appears. If needed, see Chapter 4, “OSD for All User Types” in the *AlterPath OnSite Administrator’s and User’s Guide* for details about using the OSD.

▼ To Configure Basic Network Parameters Using the OSD

1. Turn on the monitor that is connected to the Local User video port on the OnSite.
2. Enter “admin” as the Login name.
3. Enter the “cyclades” as the Password.

   If you are logging in as admin, the OSD Main Menu appears.
4. Change the admin password.

Note: Changing the default password closes a security hole that could be easily exploited.

---

   a. Go to Configure>Users and Groups>Local Users> Change Password from the OSD Main Menu.
   b. Select the admin username.
   c. Enter the password and confirm the new password.
5. Go to Configure>Network from the OSD Main Menu.

Note: See the OSD chapter in the *AlterPath OnSite Administrator’s and User’s Guide* for details.

---

   a. Disable DHCP by selecting “disabled.”
   b. Enter a static IP address for the OnSite.
   c. Enter a netmask (if needed).

   d. Enter a gateway IP address.
   e. Enter a DNS server IP address.
   f. Enter a domain name.
   g. Enter the OnSite’s hostname.
   h. Select “Save.”

6. Go to: “Selecting a Security Profile, Adding Users and Configuring Devices Using the Web Manager” on page 58.”

▼ 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 OnSite by a DHCP server.

1. Use the OnSite’s dynamically-assigned IP address in a browser to bring up the Web Manager.
2. Finish configuring users and to the OnSite using the Web Manager.
3. Make sure that the root user changes the password by logging into the OnSite console.

   See “To Change Root’s Password” on page 57.

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

The default IP address for the OnSite is `192.168.160.10`. This procedure assumes that you are able to temporarily change the IP address of a computer that has a network route to the OnSite.

1. Change the network portion of the IP address of the computer to `192.168.160` and make sure that the host portion of the IP address is not the same as the OnSite’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 OnSite'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 OnSite's IP address to a fixed public IP address and to configure the other basic network parameters.
4. Restore the computer to its previous IP address.
5. Make sure that the root user changes the root password by logging into the OnSite console.

   See "To Change Root's Password" on page 57.

Changing Root's Password

The root user must always log into the OnSite 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 or OSD to change the root password. The following options are available:

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

  If the `wiz` command is used for basic configuration, the root password should be changed (as in Step 3 in "To Configure Basic Network Parameters Using the wiz Command" on page 52).
- After an IP address is available for the OnSite, the remote root user can use `ssh` to connect to the OnSite console and log in from a remote location and change the password.

See the following procedure.

▼ To Change Root's Password

1. Connect to the OnSite's console
2. When prompted, login as root.

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

The default password is “cyclades.”

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

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

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

To complete configuration, the admin user can connect to the Web Manager by entering the IP address of the OnSite in a supported browser. For the configuration tasks the administrator needs to perform, see the *AlterPath OnSite Administrator’s and User’s Guide*. These tasks include:

- Changing the admin password.
- Selecting a security profile
- Adding users and authorizing them for access to devices by configuring their access to ports and authorizing them for managing outlets on IPDUs.
- Configuring serial ports with the appropriate settings and connection protocols to match the connected devices, and configure authentication, as desired.
- Enabling and configuring authentication and power management for KVM ports, as desired.

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

Order of installation is important, as described here:

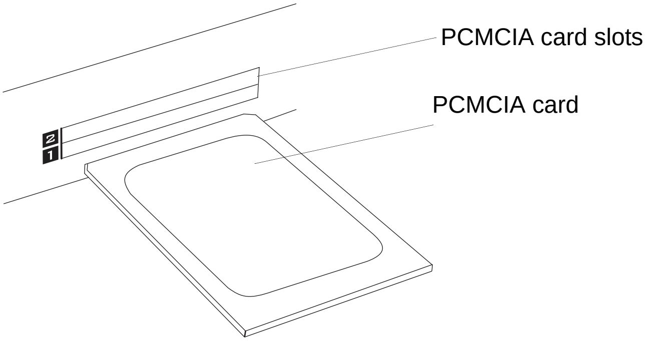
- Two PCMCIA cards of different types can be installed in any order.
- Two PCMCIA cards of the same type must be installed in the following order:
  - Insert and configure the first card in slot 1.
  - Insert and configure the second card in slot 2.

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 61 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 OnSite User’s and Administrator’s 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 60 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 60.)
   - **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 OnSite, 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 61, if needed.

   b. Insert and configure the new card.

      See “To Install a Single PCMCIA Card” on page 60 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 60 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 61, 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 60 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.

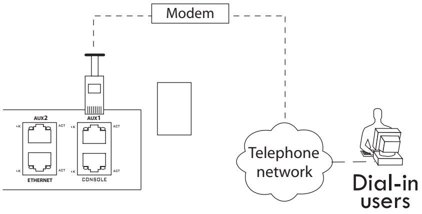


Figure 3-1: Connecting an External Modem to the AUX Port and to the Telephone Network

▼ *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) for the modem 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 OnSite.
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 OnSite User's and Administrator's Guide* for details about configuring the AUX port.

Connecting a PCMCIA Modem Card to a Phone Line

A PCMCIA modem can be connected to a dedicated phone line for dial-in access over a PPP connection or through login from a terminal emulation program. The following figure illustrates connecting a PCMCIA modem card to the telephone network.

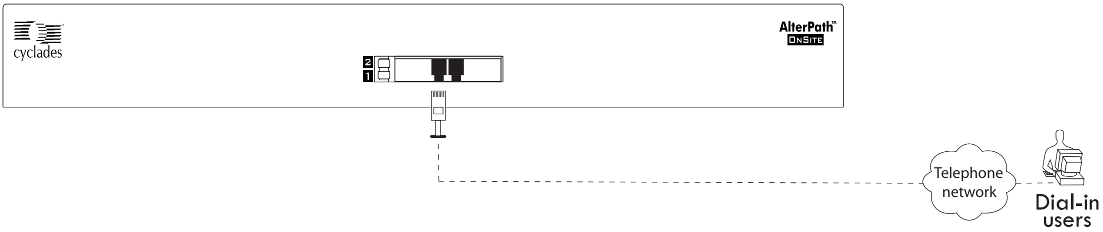


Figure 3-2: Connecting a PCMCIA Modem Card to the Telephone Network

▼ *To Connect a PCMCIA Modem Card to a Phone Line*

This procedure requires a phone cord (for connecting the modem to a live phone line) with RJ-11 connectors on both ends.

1. Connect the phone cord between the jack on the modem card and a live telephone jack at your site.
2. Configure the AUX port for PPP.

   See the *AlterPath OnSite User's and 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. See "IPDU Power Management Options" on page 13 for background details and an illustration.

Note: Do not plug the OnSite into an IPDU that is connected to the OnSite's 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 OnSite.
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 OnSite" on page 65.
3. Configure the AUX port for Power Management.

   See the *AlterPath OnSite User's and Administrator's Guide* for details about configuring the AUX port.

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

This procedure assumes that one AlterPath PM is connected to the AUX port on the OnSite. 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 OnSite.
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 OnSite User's and 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 OnSite along with its operating features and certifications.

Physical Specifications

The following table lists the OnSite's physical specifications.

Table A-1: Physical Specifications

CPU	MPC859PZP133A (PowerPC dual-CPU)
Memory	128 MByte SDRAM/128 MByte Flash
Interfaces	• 1 Ethernet 10/100BT on RJ-45 • 1 RS232 console on RJ-45 • 2 RS232 DTE on RJ-45 for power manager or external modem • 1 V.92 internal modem on DB-9 • 4 or 8 RS232 serial ports on DB-9 • 4 or 8 KVM ports on RJ-45
Dual 32/16 bit PCMCIA Slots Supporting:	Supported PCMCIA card types: • Modem • ISDN (Integrated Services Digital Network) • GSM (Global Systems for Mobile communications)/GPRS) • GPR5 • CDMA • 10/100 BaseT Ethernet • Fibre Optic Ethernet • Compact Flash • Wireless Ethernet • IDE hard disk
Dimensions (WxDxH)	(WxDxH): 17 x 10.5 x 1.75 in 43.28 x 26.25 x 4.45 cm

Table A-1: Physical Specifications (Continued)

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
Power	Universal AC, 100-240 VAC • 50/60Hz in US • 1.4 A max • Configured with other power for other countries.

Operating Features

The following table lists the OnSite'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] PAP/CHAP authentication (for dial-in lines) Token-based secure identification (RSA SecurID) IPSec support Callback support IP packet and security filtering User access lists System event syslog
User Interface	Web Manager (HTTP/HTTPS) Configuration wizard for first time configuration Command line interface (Linux shell) 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 IPDUs

Table A-2: Operating Features (Continued)

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 OnSite'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

B
Safety Information

Follow the safety 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 67 for specific standards and compliance information for the AlterPath OnSite.

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 `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* should not 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 OnSite 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 OnSite supports IPMI version 1.5. OnSite 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 OnSite 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 OnSite 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 OnSite user activates Native IP for a service processor, the OnSite 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 OnSite’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 OnSite 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.Also provided in most Cyclades products are *security profiles*.

security profiles

Most Cyclades products require the administrator to select a security profile during initial configuration, which helps enforce the security policies of the organization where the unit is being used. The security profiles are configurable and control which network services are turned on, whether a default authentication method is specified for all subsequently-configured devices, whether authorizations are checked. (Bypassing authorizations is not available in any of the default security profiles but can be selected in a custom security profile.) The security profile chosen during initial configuration can be changed later. Services can also be turned on and off independently from the security profile.

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 OnSite 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 OnSite, once a device's SoL Ethernet port is connected to one of the OnSite'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 OnSite 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 OnSite 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 OnSite. THe OnSite 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 OnSite can enter an OnSite-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