

AlterPath KVM/net Installation, Configuration, and Users Guide

Software Version 2.0



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: June 2005
Part Number: PAC0368

©2005 Cyclades Corporation

This document contains proprietary information of Cyclades Corporation and is not to be disclosed or used except in accordance with applicable contracts or agreements.

Information in this document is subject to change without notice.

All trademarks, trade names, logos and service marks referenced herein, even when not specifically marked as such, belong to their respective companies and are not to be considered unprotected by law.

The following are registered or registration-pending trademarks of Cyclades Corporation: Cyclades and AlterPath.

ActiveX, Microsoft, Microsoft Internet Explorer, Windows, and Windows NT are registered trademarks of Microsoft Corporation in the United States and other countries.

AIX is a registered trademark of International Business Machines Corporation in the United States and other countries.

FreeBSD is a registered trademark of the FreeBSD Foundation.

HP/UX is a registered trademark of the Hewlett Packard Corporation.

Linux is a registered trademark of Linus Torvalds in the United States and other countries.

Mozilla and Mozilla Firefox are trademarks of the Mozilla Foundation.

Sun, Sun Microsystems, Java, J2SE, Solaris, are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries.

UNIX is a registered trademark of The Open Group in the United States and other countries.

All rights reserved. This document may not, in whole or part, be copied, photocopied, reproduced, translated, or converted to any electronic or machine-readable form without the prior written consent of Cyclades Corporation.

Contents

Chapter 1: Introduction

Description	2
What's New in KVM/net	4
In-band Server Access	4
Color OSD	5
Enhanced Power Management for Cascaded Devices	6
Enhanced Syslogging	6
Guidelines for Using the KVM/net	6
Connectors on the KVM/net	7
Types of Ports	7
Connectors on the Back	9
Power Connector and Power Switch	10
KVM Ports	10
Management Ports (Console, Ethernet, User 1, User 2)	11
AUX Port	13
Activity LEDs on the Back of the KVM/net	13
AlterPath KVM/net Ordering Options	16
Types of Users	16
Simultaneous KVM/net Logins	17
Simultaneous Server Connections	18
Administration Options	20
Cyclades Web Manager	21
Prerequisites for Using the Web Manager	22
TCP Ports	23
Cascaded Devices	24
KVM/net Port Permissions	26
Understanding KVM Port Permissions	27
KVM Port Permissions Hierarchy	28
Decision 1: Check User's KVM Port Permissions	28
Decision 2: Check Group's KVM Port Permissions	29

Contents

Decision 3: Check Generic User's KVM Port Permissions	29
Decision 4: Check User's Default Permissions	30
Decision 5: Check Group's Default Permissions	30
Decision 6: Check Generic User's Default Permissions	31
Server Access: In-band and Out of Band	31
Determining the Connection Type and its Supported Functionality ...	
33	
Administering Users of Connected Servers	35
Types of Access to Ports	35
Tasks Related to Access to Connected Devices	35
Redefining Keyboard Shortcuts (Hot Keys)	37
Redefining KVM Connection Hot Keys	37
Redefining Sun Keyboard Equivalent Hot Keys	37
Summary of Tasks for Redefining Hot Keys	38
Packet Filtering on the KVM/net	39
Power Management	41
Setting Up and Configuring Power Management	42
Options for Managing Power	43
Controlling Power Through the Web Manager IPDU Power	
Management Forms	43
Controlling Power While Connected to KVM Ports	44
Security	44
Encryption	44
Authentication	44
Choosing Among Authentication Methods	45
Tools for Specifying Authentication Methods	47
Notifications, Alarms, and Data Buffering	48
Syslog Servers	49
Prerequisites for Logging to Syslog Servers	49
Facility Numbers for Syslog Messages	49
Example of Using Facility Numbers	49
Configuring Logging and Alarms	50
Considerations When Choosing Whether to Enable DHCP	50
KVM Terminator Usage and Types	51
KVM Expander	52
KVM Expander Features	53
KVM Expander Models and Components	54

Ports on the KVM Expander	55
LEDs on the KVM Expander	56
Power Outlets on the KVM Expander	56
Cascading a KVM Expander	56
Adding the KVM Expander to the KVM/net Unit's List of Cascaded Devices	59
Upgrading the KVM Expander Microcontroller Code	59
User Access	60
AlterPath KVM RP	61
Connectors on the Back of the KVM RP	61

Chapter 2: Installing the KVM/net

Shipping Box Contents AlterPath KVM/net	65
Setting Up the KVM/net	67
▼ To Mount the KVM/net	67
Making an Ethernet Connection	69
▼ To Make an Ethernet Connection	69
Connecting Servers to the KVM Ports	70
▼ To Prepare to Connect Devices to the KVM/net	71
▼ To Connect Computers to KVM Ports	72
Making a Direct Connection for Network Configuration	74
▼ To Connect to the Console Port	74
▼ To Connect to the User 1 Management Port	75
Powering On the KVM/net and Connected Devices	75
▼ To Power On the KVM/net	75
▼ To Power On Connected Devices	75
Performing Basic Network Configuration	76
Configuring Basic Networking Using the wiz Command	77
▼ To Log Into the KVM/net Through the Console	77
▼ To Change the Password Through the Console	77
▼ To Use the wiz Command to Configure Network Parameters	78
▼ To Apply and Confirm the Network Parameters Defined Using the wiz Command	79
Configuring Basic Networking Using the OSD	80
▼ To Log Into the OSD	81
▼ To Change a Password Using the OSD	82

Contents

▼ To Configure Network Parameters Using the OSD	84
▼ To Set the Time and Date Using the OSD	87
Completing Configuration Using the Web Manager	89
Changing Default Passwords	90
▼ Changing admin's Default Password [Web Manager]	90
▼ Changing the Root Password [Command Line]	90
▼ Changing Default Passwords [OSD]	91
Enabling Access to the Web Manager without Making a Direct Connection	92
▼ To Use the Default IP Address to Access the Web Manager	92
▼ To Use a Dynamic IP Address to Access the Web Manager	93
Preconfiguring the KVM/net for Remote Installation	95
▼ To Preconfigure the KVM/net	95
▼ To Set Up a Preconfigured KVM/net	95
Additional Configuration Tasks	96
Avoiding Conflicting Mouse Settings	96
▼ To Prevent Mouse Conflicts [Windows XP/Windows 2003]	97
▼ To Prevent Mouse Conflicts [Windows 2000 / ME]	98
▼ To Prevent Mouse Conflicts [Windows 95/98/NT]	98
▼ To Prevent Mouse Conflicts [Linux]	99
Avoiding Internet Explorer Conflicts	100
▼ To Modify IE Security Settings	100
Connecting an External Modem	103
▼ To Connect an External Modem to the AUX Port	103

Chapter 3: Installing KVM/net-related Products and Components

Connecting AlterPath PMs to the KVM/net	106
▼ To Connect a PM to the AUX Port	106
▼ To Connect Multiple PMs to the KVM/net	107
Installing the AlterPath KVM Expander	108
Shipping Box Contents KVM Expander	109
Setting Up the KVM Expander	111
▼ To Mount the KVM Expander	111
Powering On the KVM Expander and Connected Devices	114
▼ To Power On the KVM Expander	114

- ▼ To Power On Devices Daisy Chained to the KVM Expander's Power Outlet 114
 - ▼ To Power On KVM-connected Devices 114
- Connecting Cascaded KVM Units to the Primary KVM/net 115
 - ▼ To Connect a Secondary KVM, KVM/net, or KVM/net Plus to the Primary KVM/net 116
 - ▼ To Connect a KVM Expander to the Primary KVM/net 117
- Installing the AlterPath KVM Remote Presence 118
 - Shipping Box Contents KVM RP 119
 - ▼ To Connect the RP to the KVM/net 120
 - Options for Accessing the RP 120
 - ▼ To Connect the RP to a Dedicated Keyboard, Monitor, and Mouse 120
 - ▼ To Connect the RP to the Local Work Station 121
 - Supplying Power to the RP 121
 - ▼ To Power On the KVM RP 121

Chapter 4: Web Manager for Administrators

- Common Tasks 124
- Common Features of Administrators' Windows 126
 - Administrators' Control Buttons, Logout Button, and KVM/net Information 126
 - Obtaining More Information 127
- Logging Into the Web Manager and Saving Changes 128
 - ▼ To Log Into the Web Manager as Admin 128
 - ▼ To Save Configuration Changes 130
- Administrative Modes 131
- Wizard Mode 131
 - Procedures in Wizard Mode 132
 - Steps in Wizard Mode 132
 - Step 1: Network Settings [Wizard] 132
 - ▼ To Change Network Settings [Wizard] 133
 - Step 2: Access [Wizard] 134
 - ▼ To Add a User [Wizard] 135
 - ▼ To Delete a User [Wizard] 137
 - ▼ To Change a Password [Wizard] 137

Contents

Step 3: System Log [Wizard]	139
▼ To Add a Syslog Server [Wizard]	140
▼ To Delete a Syslog Server [Wizard]	140
Expert Mode	141
Overview of Menus and Forms in Expert Mode	142
Access	143
Connect to Server	143
Power Management	144
Outlets Manager	145
▼ To View Status, Lock, Unlock, and Cycle Power Outlets [Expert]	146
View IPDUs Info	147
▼ To View and Reset IPDU Information [Expert]	147
Users Manager	148
▼ To Configure Users to Manage Specific Power Outlets	148
Configuration	149
▼ To Configure Creation of Alarms and Syslog Files for IPDUs	
[Expert] 150	
Software Upgrade	150
▼ To Upgrade Firmware on an AlterPath PM [Expert]	151
Configuration	153
KVM	154
General	154
General	155
Enabling Direct Access to KVM Ports [Expert]	156
▼ To Enable Direct Access to KVM Ports [Expert]	156
Redefining KVM Connection Keyboard Shortcuts (Hot Keys) 156	
▼ To Redefine KVM Session Keyboard Shortcuts [Expert]	157
Specifying Authentication for KVM Port Logins	158
▼ To Specify an Authentication Method for KVM Port Logins	158
Local User and IP Users	159
▼ To Configure Local User 1 and User 2 Sessions	162
▼ To Configure IP User (KVM Over IP) Sessions [Expert]	163
Modifying Individual KVM Ports	164
▼ To Configure a KVM Port for Power Management [Expert] 165	
Configuring Cascaded KVM Units	166

▼ To Add a Secondary KVM Unit to be Cascaded from the Master KVM/net	167
▼ To Edit the Configuration of a Cascaded KVM Unit	168
▼ To Delete the Configuration of a Cascaded KVM Unit	170
Modifying Individual KVM Ports	170
▼ To Configure a KVM Port for Power Management [Expert]	172
▼ To Specify or Change the Alias for a KVM Port	174
▼ To Enable or Disable a KVM Port	174
Users & Groups	175
▼ To Add a User [Expert]	176
▼ To Delete a User or Group [Expert]	177
▼ To Change a User's Password [Expert]	177
▼ To Add a Group [Expert]	178
▼ To Modify a Group [Expert]	178
▼ To Select Users and Groups for Assigning KVM Port Access [Expert]	179
▼ To Assign KVM Port Access to a User or Group	180
Security	183
▼ To Configure Encryption on Port Connections [Expert]	184
Configuring an Authentication Method	185
▼ To Configure an Authentication Method for KVM/net Logins	186
▼ To Configure an Authentication Method for Logins Through KVM Ports	187
Configuring Authentication Servers for Logins to the KVM/net and Connected Devices	188
▼ To Identify a Kerberos Authentication Server	189
▼ To Identify an LDAP Authentication Server [Expert]	191
▼ To Configure an SMB(NTLM) Authentication Server [Expert]	193
▼ To Configure a NIS Authentication Server [Expert]	194
▼ To Identify a RADIUS Authentication Server [Expert]	195
▼ To Identify a TACACS+ Authentication Server [Expert]	196
Configuring In-band (RDP) Servers	197
Prerequisites for In-band Access to RDP Servers	198
▼ To Add or Modify an In-band (RDP) Server	199
▼ To Delete an In-band (RDP) Server	202
Network	203

Contents

Host Settings	204
▼ To Configure Host Settings [Expert]	205
Syslog	207
▼ To Configure Syslogging for KVM Ports and Specify Message Filtering [Expert]	208
Services	209
▼ To Select the Daemons Used for Incoming Connections	210
IP Filtering	210
▼ To Add a Chain [Expert]	218
▼ To Edit a Chain [Expert]	218
▼ To Edit a Rule for IP Filtering	219
▼ To Add a Packet Filtering Rule [Expert]	220
▼ To Add a Chain for IP Filtering	220
▼ To Edit A Chain for IP Filtering	222
▼ To Add a Rule for IP Filtering	222
VPN	227
▼ To Configure VPN	228
SNMP	231
▼ To Configure SNMP	231
Host Tables	235
▼ To Configure Hosts	235
Static Routes	237
To Add, Edit, or Delete a Static Route	237
AUX Port	239
▼ To Configure the AUX Port for Use With a PM or an External Modem	240
System	241
Time/Date	242
▼ To Set the KVM/net's Date and Time Manually	243
▼ To Set The Time and Date With NTP	243
▼ To Set the Time and Date to the KVM/net's Local GMT	244
Boot Configuration	244
▼ To Configure KVM/net Boot	248
Viewing System Information	249
General	249
▼ To View General Information for Your KVM/net	249

Port Status	250
▼ To View Port Status	250
Management	252
Backup Configuration	253
▼ To Back Up or Retrieve KVM/net Configuration Data	255
Firmware Upgrade	256
▼ To Find the Cyclades Pathname for Firmware or Microcode Upgrades 258	
▼ To Upgrade Firmware [Expert]	259
Microcode Upgrade	260
▼ To Download Microcode From an FTP Server [Expert]	261
Microcode Reset	263
▼ To Reset the Microcode After Upgrade	263
Active Sessions	264
▼ To View Active Sessions Information	264
▼ To Kill an Active Session	265
Reboot	266
▼ To Reboot the KVM/net From a Remote Location	266

Chapter 5: Web Manager for Regular Users

Web Manager for Regular Users	268
Prerequisites for Logging in to the Web Manager	270
▼ To Log Into the KVM/net Web Manager as a Regular User	270
Power Management for Regular Users	273
Power Control of Any Device Plugged Into a PM on the KVM/net ... 273	
Changing Your KVM/net Password	274
▼ To Change Your KVM/net Password	274

Chapter 6: Accessing Connected Devices

Who Can Access Connected Devices	276
Server Connections: What You See	277
Viewing KVM Connections	278
Viewing In-band Connections	280
Prerequisites for Accessing Servers With In-band Connections	280

Contents

Prerequisites for Accessing Servers With KVM Connections	281
Web Manager Login Screen	281
Login Screen: Direct Logins Not Enabled	283
Login Screen: Direct Logins Enabled, Only IP Address Entered ..	284
Login Screen: Direct Logins Enabled, IP Address and Port Entered ..	284
Connecting to Servers Remotely Through the Web Manager	286
Identifying Servers and their Connection Type in the Connect to Server Drop-down List	287
Reading the Port Numbers of Cascaded KVM Devices	288
▼ To Connect to a KVM Port Through the Login Screen	288
▼ To Connect to Servers Through The Web Manager's Connect To Server Form	290
Connecting to Servers Locally Through the OSD	292
▼ To Connect to Servers Through the OSD Connection Menu	293
Controlling KVM Port Connections	294
Hot Keys for KVM Connections	295
Hot Keys for Emulating Sun Keyboard Keys	296
▼ To Return to the Connection Menu After Connecting to a Port	297
▼ To View Connected Port Information	297
Cycling Between Servers	298
▼ To Initiate Cycle by Server	298
▼ To Connect to the Next Authorized Server from the Current Server	299
▼ To Connect to the Previous Authorized Server from the Current Server	299
▼ To Adjust Screen Brightness and Contrast	299
Resetting the Keyboard and Mouse	300
▼ To Reset the Keyboard and Mouse	300
Controlling Power of a KVM-connected Server	301
▼ To Power On, Power Off, or Reboot the Connected Server	301
Closing a KVM Connection	302
▼ To Close a KVM Connection	302
Sharing KVM Port Connections	303
AlterPath Viewer Settings	305
Recommended Settings	305
Options Menu	306

Setting the Viewer Options	307
Connection Menu	308
Power Management	309
▼ To Power On, Power Off, Lock, Unlock, or Cycle Devices Plugged into PM Outlets 310	
Modem Connections	312
▼ To Configure a PPP Connection on a Remote Computer	313
▼ To Make a PPP Connection From a Remote Computer	314

Chapter 7: On Screen Display

Navigating the OSD	318
Basic Navigation Keys	318
Common Navigation Actions	319
Logging In Through the OSD	319
▼ To Log In to the KVM/net Through the OSD	320
OSD Main Menu	320
Connection Menu	321
Power Management Menu	322
▼ To Power On, Power Off, Lock, Unlock, or Cycle Devices Plugged into PM Outlets 322	
Configure Menu Overview	323
Understanding OSD Configuration Screen Series	326
General Configuration Screens [OSD]	327
Network Configuration Menu Options [OSD]	330
Network Configuration Screens [OSD]	331
SNMP Configuration Screens [OSD]	334
VPN Configuration Screens [OSD]	338
IP Filtering Configuration Screens	342
Hosts Configuration Screens [OSD]	349
Static Routes Configuration Screens	350
Date/time Configuration Screens	353
User Station Screens	354
KVM Ports Screens	358
AUX Port Screens	359
Cascade Devices	362
Users and Groups Screens	366

Contents

Syslog Screens	373
Authentication Screens	374
Save/Load Configuration Screens	382
System Info Menu	385
▼ To Access System Information	386
Reboot	386
▼ To reboot the KVM/net	386
Controlling the OSD Through the AlterPath Remote Presence	387
▼ To Use to the AlterPath KVM RP to Access the KVM/net	387
▼ To Switch the RP Video Display from the OSD to the Local Computer 388	
▼ To Switch the RP Video Display from the Local Computer to the OSD 388	
▼ To Turn the Beeper On or Off When Switching Between the Local and the Remote Work Stations 389	

Chapter A: Troubleshooting

Replacing a Boot Image	392
Downloading a New Software Version	393
Changing the Boot Image	394
▼ To Boot from an Alternate Image With bootconf	394
Changing the Boot Image in U-Boot Monitor Mode	395
▼ To Boot in U-Boot Monitor Mode	396
▼ To Boot from an Alternate Image in U-Boot Monitor Mode	396
▼ To Boot in Single User Mode from U-Boot Monitor Mode	397
▼ To Replace a Boot Image From a Network Boot in U-Boot Monitor Mode 397	
▼ To Restore the KVM/net Configuration to the Factory Default	398

Glossary	399
-----------------------	------------

Index	407
--------------------	------------

Contents

List of Procedures

▼ To Mount the KVM/net.....	67
▼ To Make an Ethernet Connection.....	69
▼ To Prepare to Connect Devices to the KVM/net.....	71
▼ To Connect Computers to KVM Ports.....	72
▼ To Connect to the Console Port	74
▼ To Connect to the User 1 Management Port	75
▼ To Power On the KVM/net	75
▼ To Power On Connected Devices	75
▼ To Log Into the KVM/net Through the Console.....	77
▼ To Change the Password Through the Console	77
▼ To Use the wiz Command to Configure Network Parameters.....	78
▼ To Apply and Confirm the Network Parameters Defined Using the wiz Command	79
▼ To Log Into the OSD.....	81
▼ To Change a Password Using the OSD.....	82
▼ To Configure Network Parameters Using the OSD	84
▼ To Set the Time and Date Using the OSD	87
▼ Changing admin's Default Password [Web Manager].....	90
▼ Changing the Root Password [Command Line].....	90
▼ Changing Default Passwords [OSD].....	91
▼ To Use the Default IP Address to Access the Web Manager.....	92
▼ To Use a Dynamic IP Address to Access the Web Manager	93
▼ To Preconfigure the KVM/net.....	95
▼ To Set Up a Preconfigured KVM/net.....	95
▼ To Prevent Mouse Conflicts [Windows XP/Windows 2003]	97

List of Procedures

▼ To Prevent Mouse Conflicts [Windows 2000 / ME].....	98
▼ To Prevent Mouse Conflicts [Windows 95/98/NT]	98
▼ To Prevent Mouse Conflicts [Linux]	99
▼ To Modify IE Security Settings	100
▼ To Connect an External Modem to the AUX Port.....	103
▼ To Connect a PM to the AUX Port	106
▼ To Connect Multiple PMs to the KVM/net.....	107
▼ To Mount the KVM Expander	111
▼ To Power On the KVM Expander.....	114
▼ To Power On Devices Daisy Chained to the KVM Expander's Power Outlet.....	114
▼ To Power On KVM-connected Devices.....	114
▼ To Connect a Secondary KVM, KVM/net, or KVM/net Plus to the Primary KVM/net.....	116
▼ To Connect a KVM Expander to the Primary KVM/net	117
▼ To Connect the RP to the KVM/net.....	120
▼ To Connect the RP to a Dedicated Keyboard, Monitor, and Mouse	120
▼ To Connect the RP to the Local Work Station.....	121
▼ To Power On the KVM RP	121
▼ To Log Into the Web Manager as Admin	128
▼ To Save Configuration Changes	130
▼ To Change Network Settings [Wizard].....	133
▼ To Add a User [Wizard].....	135
▼ To Delete a User [Wizard]	137
▼ To Change a Password [Wizard].....	137
▼ To Add a Syslog Server [Wizard].....	140
▼ To Delete a Syslog Server [Wizard]	140
▼ To View Status, Lock, Unlock, and Cycle Power Outlets [Expert].....	146
▼ To View and Reset IPDU Information [Expert]	147

▼ To Configure Users to Manage Specific Power Outlets	148
▼ To Configure Creation of Alarms and Syslog Files for IPDUs [Expert].....	150
▼ To Upgrade Firmware on an AlterPath PM [Expert].....	151
▼ To Enable Direct Access to KVM Ports [Expert]	156
▼ To Redefine KVM Session Keyboard Shortcuts [Expert]	157
▼ To Specify an Authentication Method for KVM Port Logins	158
▼ To Configure Local User 1 and User 2 Sessions	162
▼ To Configure IP User (KVM Over IP) Sessions [Expert]	163
▼ To Configure a KVM Port for Power Management [Expert]	165
▼ To Add a Secondary KVM Unit to be Cascaded from the Master KVM/net.....	167
▼ To Edit the Configuration of a Cascaded KVM Unit.....	168
▼ To Delete the Configuration of a Cascaded KVM Unit.....	170
▼ To Configure a KVM Port for Power Management [Expert]	172
▼ To Specify or Change the Alias for a KVM Port.....	174
▼ To Enable or Disable a KVM Port.....	174
▼ To Add a User [Expert].....	176
▼ To Delete a User or Group [Expert].....	177
▼ To Change a User's Password [Expert]	177
▼ To Add a Group [Expert]	178
▼ To Modify a Group [Expert]	178
▼ To Select Users and Groups for Assigning KVM Port Access [Expert]	179
▼ To Assign KVM Port Access to a User or Group	180
▼ To Configure Encryption on Port Connections [Expert]	184
▼ To Configure an Authentication Method for KVM/net Logins	186
▼ To Configure an Authentication Method for Logins Through KVM Ports	187
▼ To Identify a Kerberos Authentication Server	189
▼ To Identify an LDAP Authentication Server [Expert].....	191

List of Procedures

▼ To Configure an SMB(NTLM) Authentication Server [Expert] ...	193
▼ To Configure a NIS Authentication Server [Expert]	194
▼ To Identify a RADIUS Authentication Server [Expert].....	195
▼ To Identify a TACACS+ Authentication Server [Expert]	196
▼ To Add or Modify an In-band (RDP) Server	199
▼ To Delete an In-band (RDP) Server	202
▼ To Configure Host Settings [Expert]	205
▼ To Configure Syslogging for KVM Ports and Specify Message Filtering [Expert].....	208
▼ To Select the Daemons Used for Incoming Connections	210
▼ To Add a Chain [Expert].....	218
▼ To Edit a Chain [Expert]	218
▼ To Edit a Rule for IP Filtering	219
▼ To Add a Packet Filtering Rule [Expert]	220
▼ To Add a Chain for IP Filtering	220
▼ To Edit A Chain for IP Filtering	222
▼ To Add a Rule for IP Filtering	222
▼ To Configure VPN	228
▼ To Configure SNMP	231
▼ To Configure Hosts	235
▼ To Configure the AUX Port for Use With a PM or an External Modem.....	240
▼ To Set the KVM/net's Date and Time Manually	243
▼ To Set The Time and Date With NTP	243
▼ To Set the Time and Date to the KVM/net's Local GMT	244
▼ To Configure KVM/net Boot	248
▼ To View General Information for Your KVM/net.....	249
▼ To View Port Status	250
▼ To Back Up or Retrieve KVM/net Configuration Data	255

▼ To Find the Cyclades Pathname for Firmware or Microcode Upgrades	258
▼ To Upgrade Firmware [Expert]	259
▼ To Download Microcode From an FTP Server [Expert]	261
▼ To Reset the Microcode After Upgrade	263
▼ To View Active Sessions Information	264
▼ To Kill an Active Session	265
▼ To Reboot the KVM/net From a Remote Location	266
▼ To Log Into the KVM/net Web Manager as a Regular User	270
▼ To Change Your KVM/net Password	274
▼ To Connect to a KVM Port Through the Login Screen	288
▼ To Connect to Servers Through The Web Manager's Connect To Server Form	290
▼ To Connect to Servers Through the OSD Connection Menu	293
▼ To Return to the Connection Menu After Connecting to a Port	297
▼ To View Connected Port Information	297
▼ To Initiate Cycle by Server	298
▼ To Connect to the Next Authorized Server from the Current Server	299
▼ To Connect to the Previous Authorized Server from the Current Server	299
▼ To Adjust Screen Brightness and Contrast	299
▼ To Reset the Keyboard and Mouse	300
▼ To Power On, Power Off, or Reboot the Connected Server	301
▼ To Close a KVM Connection	302
▼ To Power On, Power Off, Lock, Unlock, or Cycle Devices Plugged into PM Outlets	310
▼ To Configure a PPP Connection on a Remote Computer	313
▼ To Make a PPP Connection From a Remote Computer	314
▼ To Log In to the KVM/net Through the OSD	320
▼ To Power On, Power Off, Lock, Unlock, or Cycle Devices Plugged into PM Outlets	322

List of Procedures

▼ To Access System Information	386
▼ To reboot the KVM/net	386
▼ To Use to the AlterPath KVM RP to Access the KVM/net	387
▼ To Switch the RP Video Display from the OSD to the Local Computer	388
▼ To Switch the RP Video Display from the Local Computer to the OSD	388
▼ To Turn the Beeper On or Off When Switching Between the Local and the Remote Work Stations	389
▼ To Boot from an Alternate Image With bootconf	394
▼ To Boot in U-Boot Monitor Mode	396
▼ To Boot from an Alternate Image in U-Boot Monitor Mode	396
▼ To Boot in Single User Mode from U-Boot Monitor Mode	397
▼ To Replace a Boot Image From a Network Boot in U-Boot Monitor Mode	397
▼ To Restore the KVM/net Configuration to the Factory Default ...	398

List of Procedures

List of Tables

Table iv-1:	Typographic Conventions	xxxiv
Table iv-2:	Other Terms and Conventions	xxxv
Table 1-1:	Port Types	7
Table 1-2:	LED Descriptions	14
Table 1-3:	AlterPath KVM/net Model Numbers and Port Options	16
Table 1-4:	User Types, Responsibilities, and Default Password...	17
Table 1-5:	Number of Simultaneous Server Connections.....	19
Table 1-6:	Administration Options.....	20
Table 1-7:	Supported Browsers.....	22
Table 1-8:	Tasks: Configuring TCP Port Numbers and Port Aliases	23
Table 1-9:	Connectors and Ports for Cascading KVM Units.....	25
Table 1-10:	Default Port Access Permissions	26
Table 1-11:	Tools for Setting KVM Port Permissions	28
Table 1-12:	Available Functionality During KVM and In-band Connections	33
Table 1-13:	Tasks for Redefining Hot Keys.....	38
Table 1-14:	Levels of IP Filtering.....	39
Table 1-15:	Supported Authentication Types for KVM/net and Port Types.....	45
Table 1-16:	Specifying Authentication Methods	47
Table 1-17:	AlterPath KVM Terminators.....	51
Table 1-18:	KVM Expander Model Numbers and Port Options.....	54
Table 1-19:	KVM Expander Port Types.....	55
Table 1-20:	Maximum Number of Supported Servers	58

List of Tables

Table 1-21:	KVM RP Port Types	62
Table 2-1:	Shipping Box Contents, Part Numbers, and Description	65
Table 2-2:	OSD Equivalents for Common Actions.....	80
Table 3-1:	KVM Expander Shipping Box Contents, Part Numbers, and Description	109
Table 3-2:	KVM RP Shipping Box Contents, Part Numbers, and Description	119
Table 4-1:	Network Forms	203
Table 4-2:	Host Settings Configuration Fields.....	205
Table 4-3:	Add/Modify Static Routes Fields.....	238
Table 4-4:	PPP Fields for Configuring the AUX Port.....	240
Table 4-5:	Boot Configuration Fields and Options	246
Table 4-6:	Port Status Information	251
Table 5-1:	Power Management Tasks Available to Regular Users.....	273
Table 6-1:	Web Manager Login Screen Options.....	281
Table 6-2:	Tasks Available While Connected to KVM Ports.....	294
Table 6-3:	Default KVM Connection Keyboard Shortcuts.....	295
Table 6-4:	Default Sun Key Emulation Hot Keys.....	296
Table 6-5:	AlterPath Viewer>Options>Viewer Options Menu ...	307
Table 6-6:	Tasks for Configuring and Making Dial Up Connections (User)	312
Table 7-1:	Basic Navigation Keys.....	318
Table 7-2:	OSD Equivalents for Common Actions.....	319
Table 7-3:	OSD Main Menu Items.....	320
Table 7-4:	Configuration Menu Items.....	324
Table 7-5:	General Configuration Screens [OSD]	327
Table 7-6:	Network Configuration Screens [OSD].....	332
Table 7-7:	SNMP Configuration Screens [OSD]	336
Table 7-8:	VPN Configuration Screens [OSD].....	339
Table 7-9:	IP Filtering Configuration Screens [OSD].....	344

Table 7-10:	Hosts Configuration Screens [OSD].....	350
Table 7-11:	Static Routes Screens [OSD]	351
Table 7-12:	User Station Configuration Screens.....	355
Table 7-13:	KVM Port Configuration Screens.....	358
Table 7-14:	KVM Port Configuration Screens.....	360
Table 7-15:	Cascade Devices Configuration Screens	363
Table 7-16:	Local Users Configuration Screens	368
Table 7-17:	Local Groups Configuration Screens.....	369
Table 7-18:	User Access List KVM Port Permissions Configuration Screens.....	371
Table 7-19:	Authentication Configuration Screens for KVM/net Logins	376
Table 7-20:	Common Configuration Screens for Kerberos and LDAP Authentication Servers	376
Table 7-21:	Unique LDAP Authentication Server Configuration Screens	378
Table 7-22:	Configuration Screens for the Radius or TACACS+ Authentication Servers.....	379
Table 7-23:	Smb (NTLM) Configuration Screens	380
Table 7-24:	NIS Configuration Screens	381
Table 7-25:	Save/Load Configuration Screens	383
Table 7-26:	System Information Example	385
Table A-1:	Boot Partitions, Formats, and Contents	392

List of Tables

List of Figures

Figure 1-1:	KVM/net Front and Back	2
Figure 1-2:	OSD Main Menu.....	5
Figure 1-3:	KVM/net Back Panel.....	9
Figure 1-4:	Power Connector and KVM Server Ports on the Left Rear	10
Figure 1-5:	KVM Ports on the Center Rear.....	10
Figure 1-6:	Management Ports	11
Figure 1-7:	Management Ports	13
Figure 1-8:	LEDs on the KVM/net Management Ports.....	14
Figure 1-9:	Cascaded KVM Devices from an KVM/net.....	24
Figure 1-10:	Connecting an AlterPath PM to the KVM/net.....	41
Figure 1-11:	KVM Expander Back Panel Components	54
Figure 1-12:	Ports on the KVM Expander Back Panel.....	55
Figure 1-13:	Connecting a KVM Expander to the KVM/net	57
Figure 1-14:	Devices Form on KVM/net Web Manager	59
Figure 1-15:	Microcode Update Form on KVM/net Web Manager	60
Figure 1-16:	KVM RP Front.....	61
Figure 1-17:	KVM RP Back Panel	61
Figure 4-1:	Example Window in Wizard Mode.....	131
Figure 5-1:	Cyclades KVM/net Web Manager	269
Figure 6-1:	AlterPath Viewer for KVM Connections.....	278
Figure 6-2:	ActiveX Viewer for In-band Connections	280
Figure 6-3:	Web Manager Login Screen Without KVM Direct Logins Enabled	283
Figure 6-4:	AlterPath Viewer Options Screen	307
Figure 7-1:	OSD Main Menu.....	320

List of Figures

Figure 7-2:	First, Middle, and Last Screens in Configuration Series	326
Figure 7-3:	User Station Configuration Screens	355
Figure 7-4:	KVM Ports Configuration Screens	358
Figure 7-5:	AUX Port Configuration Screens	360
Figure 7-6:	Cascade Devices Configuration Screens	363
Figure 7-7:	Users and Groups Configuration Screens	367
Figure 7-8:	Syslog Configuration Server Screen	373
Figure 7-9:	Authentication Options and Screens	375
Figure 7-10:	Save/Load Config Configuration Screens	383

Before You Begin

This installation, administration, and users guide provides background information and procedures for installing, configuring, and administering the Cyclades AlterPath™ family of KVM products including:

- AlterPath KVM/net
- AlterPath KVM Expander
- AlterPath KVM RP
- AlterPath KVM Terminators

In addition, this guide offers information and procedures for accessing connected servers and other connected devices.

Audience

This manual is intended for installers and system administrators of the KVM/net and for users who may be authorized to connect to devices and to manage power through the KVM/net.

This document describes configuration, administration, and use of the KVM/net only. It does not describe how to set up and administer other external services or servers that the KVM/net may access for authentication, system logging, SNMP notifications, data logging, file sharing, or other purposes. This document assumes that users who are authorized to connect to servers and other devices through the KVM/net already know how to use the connected devices.

Document Organization

The document contains the following chapters:

Chapter 1: Introduction

Defines and explains the overall product features and uses of AlterPath KVM/net.

Chapter 2: Installing the KVM/net

Explains the procedures for installing the KVM/net and setting up its basic configuration.

Chapter 3: Installing KVM/net-related Products and Components

Explains the procedures for installing the KVM Expander and the KVM RP in addition to explaining how to install PCMCIA cards, an external modem, an AlterPath PM and how to cascade KVM units to the KVM/net.

Chapter 4: Web Manager for Administrators

Explains how to use the Web Manager, highlighting such procedures as how to configure the KVM/net, add or delete users, define user access, add or delete server connections, and other topics pertaining to KVM/net administration.

Chapter 5: Web Manager for Regular Users

Presents the procedures for connecting to a port and other operations related to using the web user interface.

Chapter 6: Accessing Connected Devices

Explains how to connect to KVM ports and in-band servers and how to use the AlterPath Viewer and control KVM connection sessions.

Chapter 7: On Screen Display	Explains how to use the On Screen display for local connections to the User 1 port, highlighting such procedures as how to configure the KVM/net, adding or deleting users, defining user access, adding or deleting server connections, and other topics pertaining to KVM/net administration.
Appendix A: Troubleshooting	Explains how to troubleshoot common KVM/net issues.
Glossary	Glossary of terms and acronyms used in the manual.

Related Documents

The following document for the Cyclades AlterPath KVM/net is shipped with the product.

- *AlterPath KVM/net Quick Start Guide* (hard-copy)

The following manuals for Cyclades AlterPath products mentioned in this guide are on the Documentation CD shipped with the product and they are also available at: <http://www.cyclades.com/support/downloads.php>.

- *AlterPath PM User Guide*
- *AlterPath Manager E2000 Manual*
- *AlterPath KVM/net Plus Installation, Configuration, and Users Guide*
- *AlterPath KVM Installation, Configuration, and Users Guide*

Updated versions of this document will be posted on the downloads section of the Cyclades website in the “AlterPath KVM/net” section when Cyclades releases new versions of the software.

A printed version of this document can be ordered under part number OST0000-U00 through your Cyclades sales representative.

Typographic and Other Conventions

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

Table iv-1: Typographic Conventions

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

The following table describes other terms and conventions.

Table iv-2:Other Terms and Conventions

Term or Convention	Meaning	Examples
Hot keys	<ul style="list-style-type: none"> 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. 	<ul style="list-style-type: none"> 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.
Navigation shortcuts	Shortcuts use the “greater than” symbol (>) to indicate how to navigate to Web Manager forms or OSD screens.	Go to Configuration>KVM> General >IP Users in Expert mode.

Before You Begin

Chapter 1

Introduction

This chapter gives an overview of the features of the Cyclades™ AlterPath™ KVM/net. This chapter describes how administrators and operators can use the KVM/net features to securely manage connected computer systems and a large variety of devices from anywhere on the local area network or on the Internet. This chapter also provides important prerequisite information for understanding the information and procedures in the rest of this manual.

Description

The KVM/net is a 1U rack-mountable device that serves as a single access point for administering and using servers and other devices through in-band and out-of-band access methods.

The following figure shows the front and back of the KVM/net.



Figure 1-1: KVM/net Front and Back

You can use the two PCMCIA card slots in the front for optional v.90 modem or secondary Ethernet PCMCIA cards.

You use the KVM ports on the left and middle back of the KVM/net to connect servers. You can use the AUX port on the right to connect AlterPath PM IPDUs or an optional external modem. You use the management ports on the right to connect to the KVM/net and to its connected devices.

Depending on the model, the KVM/net comes with either 16 or 32 KVM ports to connect from 16 to 32 servers with KVM connections.

The KVM/net can be used to manage power of up to 128 devices when the devices are plugged into up to 32 daisy-chained AlterPath PM intelligent power distribution units that are connected to the AUX port on the KVM/net.

KVM/net administrators and users who are authorized to access connected devices can connect locally or remotely from LANs, WANs, or other dial-up connections through the Ethernet port or through an optional external modem.

For extended local administration, administrators can connect the Cyclades AlterPath KVM Expander (purchased separately) to the KVM/net with a CAT5 cable of up to 500 feet in length.

Note: The 500-foot limit includes the distance of the User 2 from the KVM/net and the distance of the most remote system connected to a KVM port.

Secondary KVM units such as the Cyclades AlterPath KVM Expander or an AlterPath KVM can be cascaded for extended KVM server connections. A maximum of 32 secondary KVM devices can be cascaded from the primary KVM/net extending the number of KVM ports to a maximum of 1024.

If multiple KVM/net are installed in multiple remote locations, a Cyclades AlterPath Manager (purchased separately) can manage all the KVM/net units together with other Cyclades products and their connected devices through a single IP address.

Access to the KVM/net for administration is separate from access to connected devices. Only the KVM/net administrator can configure access to the KVM/net and to the connected devices.

Both KVM/net administrators and users authorized to access connected devices can use the Web Manager from a browser. Authorized users can log into devices, manage power, and change their own passwords, but they do not have access to the KVM/net screens for configuring users or ports.

All logins to the KVM/net are subject to authentication. The KVM/net administrator can restrict access to each of the connected devices by choosing among authentication methods for logins to the KVM/net and to its ports. Authentication can be local to the KVM/net or through an authentication server.

The KVM/net administrator can further control access by controlling which ports are assigned to each user name.

The KVM/net administrator can configure event logging, alarms, and notifications, set up encryption, and data buffering.

After initial network configuration is performed on the KVM/net, the Cyclades Web Manager provides a real-time view of all the connected equipment and makes it possible for administration to be done from a browser on any computer on site or on the Internet.

What's New in KVM/net

The KVM/net supports the following new features:

- “In-band Server Access” on page 4
- “Color OSD” on page 5
- “Enhanced Power Management for Cascaded Devices” on page 6
- “Enhanced Syslogging” on page 6

In-band Server Access

KVM/net offers in-band connections to Windows Terminal Servers that have RDP enabled. With valid IP addresses, administrators can configure as many in-band connections as they can out-of-band KVM connections without using cables, a KVM port, or a KVM Terminator. However, if desired, dual KVM and in-band access can be configured for each Windows Terminal Server.

KVM/net users can make up to eight server connections at once over the Ethernet or dial up (remote) in addition to making up to two simultaneous local KVM connections. Up to two of the remote connections can be KVM, while the rest can be in band, adding up to eight total remote connections. The following list describes the types and number of connections available to the KVM/net:

- Up to eight in-band (RDP) connections OR
- Up to two KVM over IP connections plus the number of in-band connections that add up to eight when added to the number of active KVM over IP connections AND
- Local User 1 and Local User 2 connected, independently of KVM over IP and/or in-band connections

In-band connections have faster control response times than KVM connections, and there is no need to synchronize the keyboard and mouse.

The following links offer more detailed information on in-band connections:

- See “Server Access: In-band and Out of Band” on page 36 for a description of in-band and out-of-band server access.
- See “Configuring In-band (RDP) Servers” on page 197 for instructions on configuring RDP servers for in-band access.
- See Chapter 5. “Web Manager for Regular Users” on page 267 for instructions on making in-band server connections.

Color OSD

In KVM/net, the OSD uses multiple colors to enhance its usability. A selected option is highlighted in green.

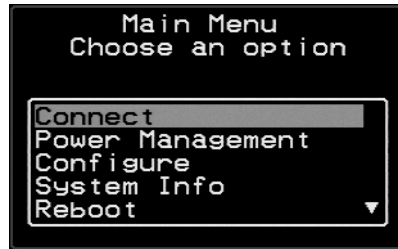


Figure 1-2: OSD Main Menu

Enhanced Power Management for Cascaded Devices

The KVM/net supports power management on devices connected to the AUX ports of cascaded KVM units. See “Power Management” on page 41 for more details.

Enhanced Syslogging

The KVM/net supports configuring a syslog server to accept and store syslog messages from the AUX and KVM ports. See “Notifications, Alarms, and Data Buffering” on page 48 for more information.

Guidelines for Using the KVM/net

Configuration of user accounts and access to the ports and all other management of the connected devices is done through the Web Manager.

Troubleshooting in the event of network failure can be done using one of the two direct-connect methods, or by using the Web Manager through a dial-up connection to an external modem connected to the AUX port.

See the “Accessing Connected Devices” on page 275 for instructions on how users without KVM/net administration privileges can access computers and AlterPath PMs that are connected to the KVM/net.

Connectors on the KVM/net

The following sections describe the connectors on the back of the KVM/net, including ports and plugs.

Types of Ports

The KVM/net's ports include KVM ports, which support server connections, an AUX port, and management ports including the User 1, User 2, Console, and Ethernet ports, as described in the following table.

Table 1-1: Port Types

Port Type	Connection Information	Where Documented
KVM	Connect an RJ-45 CAT5 Ethernet cable to a Terminator, which is connected to a USB Sun server running Solaris or a PC running a Windows, Linux, or other open source operating system.	<ul style="list-style-type: none"> • “KVM Ports” on page 10 • “To Connect Computers to KVM Ports” on page 72
AUX	Connect an RJ-45 cable to an: <ul style="list-style-type: none"> • AlterPath PM intelligent power distribution unit (IPDU) or <ul style="list-style-type: none"> • external modem. 	<ul style="list-style-type: none"> • “AUX Port” on page 13 • “To Connect a PM to the AUX Port” on page 106 • “To Connect an External Modem to the AUX Port” on page 103
Console	Connect a CAT5 to DB-9 cable to a COM port on a computer.	<ul style="list-style-type: none"> • “Management Ports (Console, Ethernet, User 1, User 2)” on page 11 • “To Connect to the Console Port” on page 74
Ethernet	Connect an Ethernet cable to the local area network (LAN).	<ul style="list-style-type: none"> • “Management Ports (Console, Ethernet, User 1, User 2)” on page 11 • “To Make an Ethernet Connection” on page 69

Table 1-1: Port Types (Continued)

Port Type	Connection Information	Where Documented
User 1 [PS/2 and VGA]	Connect a keyboard, video, mouse cable to a local station's mouse, keyboard, and monitor.	<ul style="list-style-type: none"> • “Management Ports (Console, Ethernet, User 1, User 2)” on page 11 • “To Connect to the User 1 Management Port” on page 75
User 2	<p>Connect an RJ-45 cable of up to 500 feet to an AlterPath Remote Presence (RP). The RP can be ordered separately.</p> <p>Note: The 500-foot limit includes the distance of the User 2 from the KVM/net and the distance of the most remote system connected to a KVM port.</p>	<ul style="list-style-type: none"> • “Management Ports (Console, Ethernet, User 1, User 2)” on page 11 • “AlterPath KVM RP” on page 61 • “To Connect the RP to the KVM/net” on page 120

Connectors on the Back

The back of the KVM/net has KVM and management ports, a power cord connector, a power switch, and an AUX port as illustrated in the following figure.

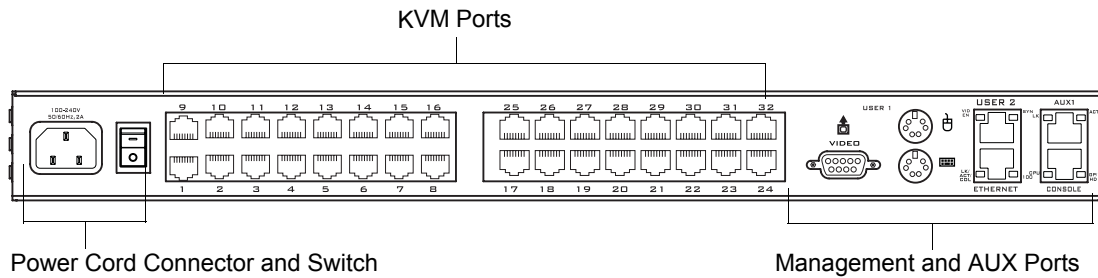


Figure 1-3: KVM/net Back Panel

- On the left are the power connector and power switch and either 16 or 32 KVM ports, which are used for connecting computing systems with KVM connections.
See “Power Connector and Power Switch” on page 10 and “KVM Ports” on page 10.
- On the right is the AUX port, which is used to connect to PMs or an external modem, and the management ports, which are used for local management of the KVM/net.
See “Management Ports (Console, Ethernet, User 1, User 2)” on page 11 and “AUX Port” on page 13.

Power Connector and Power Switch

The following figure shows the power connector and power switch on the left rear of a KVM/net.

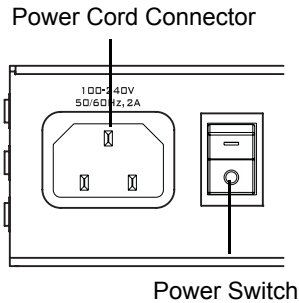


Figure 1-4: Power Connector and KVM Server Ports on the Left Rear

The KVM/net is furnished with a power cord used to connect the power connector to a power supply.

See “To Power On the KVM/net” on page 75 for instructions on supplying power to the KVM/net.

KVM Ports

The following figure shows KVM (keyboard, video, mouse) ports on the center rear of the KVM/net.

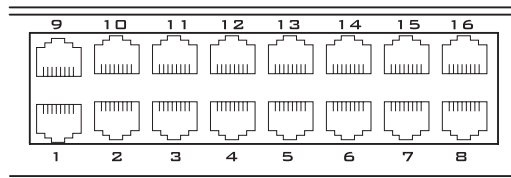


Figure 1-5: KVM Ports on the Center Rear

KVM ports provide remote access to the keyboard, monitor, and mouse of a USB Sun server running Solaris or a PC running a Windows, Linux, or other open source operating system. Connecting a computer to a KVM port allows use of a keyboard, video, and mouse from a remote station as if it were the keyboard video and mouse on the connected computer. KVM port connections, also called out-of-band connections give access to information that is otherwise inaccessible through in-band network interfaces.

For example, BIOS access, POST, and boot messages are inaccessible through in-band connections. In some cases, the in-band network interfaces are not available after the system boot is completed (for example, after a Windows Safe Mode boot) without the kind of access these KVM connections provide.

Each connected computing system is identified in the management software by the port number to which it is connected. The administrator can assign a descriptive alias to each port to identify the connected computer. For example, if a Sun E10K server is connected to port 3, the administrator might define the port's alias to be "Sun E10K."

Customers order one of three terminator types for connecting each KVM port to a computer. See "KVM Terminator Usage and Types" on page 51 for more details.

See "To Connect Computers to KVM Ports" on page 72 for instructions on connecting devices to KVM ports.

Management Ports (Console, Ethernet, User 1, User 2)

The following figure shows the management ports on the right back of the KVM/net.

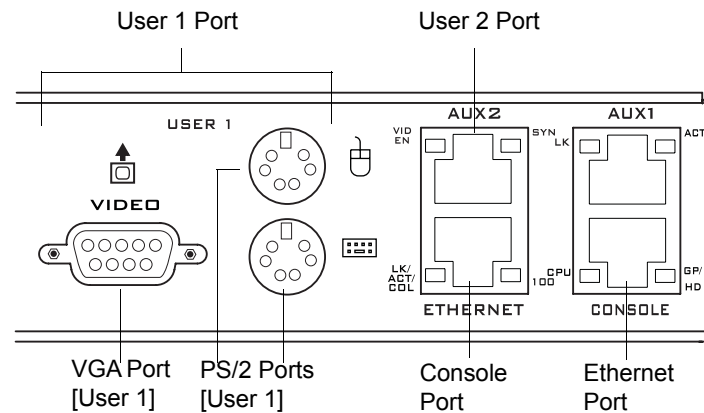


Figure 1-6: Management Ports

Introduction

The following table describes the management ports on the right back of the KVM/net.

- **Console** – Its RJ-45 connection can be connected by a CAT5 to DB-9 cable to a COM port on a computer. Administrators can use a terminal emulation program to locally manage and troubleshoot the KVM/net. See “To Connect to the Console Port” on page 74 and “Configuring Basic Networking Using the wiz Command” on page 77 for more details.
- **Ethernet** – Use the Ethernet management port for connecting an Ethernet cable for Intranet and Internet access. See “Making an Ethernet Connection” on page 69 for instructions if needed.
- **User 1** – The User 1 port includes two PS/2 ports and a VGA port, which can be connected to a mouse, keyboard, and monitor. Administrators can use the OSD (On Screen Display) to locally manage and use the KVM/net. See “To Connect to the User 1 Management Port” on page 75 and Chapter 7: On Screen Display for more details.
- **User 2** – This port is used for extending the local administration by connecting an RJ-45 cable of up to 500 feet to an AlterPath Remote Presence (RP). The RP can be ordered separately. Administrators can use the OSD (On Screen Display) to locally manage and use the KVM/net without being in the same room as the KVM/net. See “Installing the AlterPath KVM Remote Presence” on page 118 and “Controlling the OSD Through the AlterPath Remote Presence” on page 387 for more details.

AUX Port

The following figure shows the AUX port on the right back of the KVM/net.

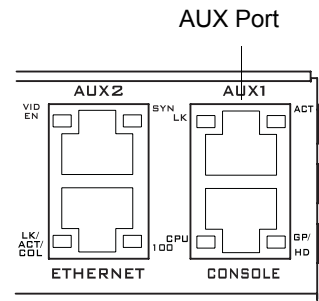


Figure 1-7: Management Ports

AUX – Its RJ45 connector can be used for the following:

- Connecting to an optional AlterPath PM IPDU
Up to 32 IPDUs can be daisy-chained for a total of 120 outlets. See “Power Management” on page 41 for background information of power management and see “Connecting AlterPath PMs to the KVM/net” on page 106 for installation instructions.
- Connecting to an optional external modem
See “Connecting an External Modem to the KVM/net Plus” on page 103

Activity LEDs on the Back of the KVM/net

The KVM/net comes with paired LEDs positioned on each side of the following ports:

- User 2
- AUX
- Ethernet
- Console

The following figure shows the position of the LEDs as they appear on the back of the KVM/net. The LEDs are designed to monitor the interface connections as described in Table 1-2, “Management Port LED Status Definitions,” on page 1-20.

Introduction

The diagram below shows a close up view of the LEDs on the back of the KVM/net. The LEDs monitor the AUX ports, ETHERNET, and CONSOLE ports as described in Table 1-2.

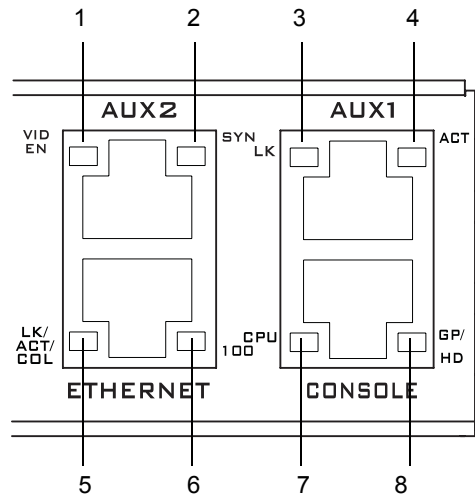


Figure 1-8: LEDs on the KVM/net Management Ports

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

Table 1-2: LED Descriptions

Number	Label	Function	Color/Status
1	VID EN	Monitor KVM CAT5 video interface	Orange – Lights when video is enabled
2	SYN	Monitor KVM CAT5 video interface	Yellow – Lights when KVM input is being transmitted through one or more KVM ports.
5, 3	LK	Monitor RS-232 async port status	<ul style="list-style-type: none"> • OFF – Indicates the port is not open. • Orange – Lights when DTR (data terminal ready) signal is on (when the port is open).

Table 1-2: LED Descriptions (Continued)

Number	Label	Function	Color/Status
4, 5	ACT	Monitor RS-232 async activity	<ul style="list-style-type: none"> • OFF – Indicates no data activity. • Green – Blinks when data is either being received (RX) or transmitted (TX).
5	LK/ ACT/ COL	Monitor Ethernet line status	<ul style="list-style-type: none"> • OFF – Indicates either link is not up or cable is not connected. • Green – Lights solid when the link is up and blinks when data activity occurs, with frequency proportional to traffic. • Orange – Blinks when collisions occur
6	100	Monitor Ethernet speed	<ul style="list-style-type: none"> • Off – Indicates the link is 10baseT or no link is active. • Green – Steady when 100baseT link is active.
7	CPU	Monitor CPU (software operation)	<ul style="list-style-type: none"> • 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 KVM/net reboots.
8	GP/ HD	Monitor compact flash (HD) or other (GP)	Not implemented.

AlterPath KVM/net Ordering Options

Each AlterPath KVM/net comes with 16 or 32 KVM ports. The following table lists the model and part numbers and number of KVM ports of each KVM unit.

Table 1-3: AlterPath KVM/net Model Numbers and Port Options

Model Number	Part Numbers	KVM Ports
16	ATP4116	16
32	ATP4132	32

Types of Users

The KVM/net support three types of users:

- Predefined administrators who can administer the KVM/net and its connected devices
- Optionally-added users who can act as administrators of the KVM/net and its connected devices
- Optionally-added users who can act as administrators of connected devices or regular users.

As summarized in the following table, two accounts, root and admin, are configured by default and cannot be deleted. The default “admin” account can add regular user accounts to allow other users to act as administrators of connected devices. An administrator can also choose to add regular users to the “admin” group, which enables the regular users to perform KVM/net

administrative functions. The following table lists the responsibilities of each type of user and provides the default password for each.

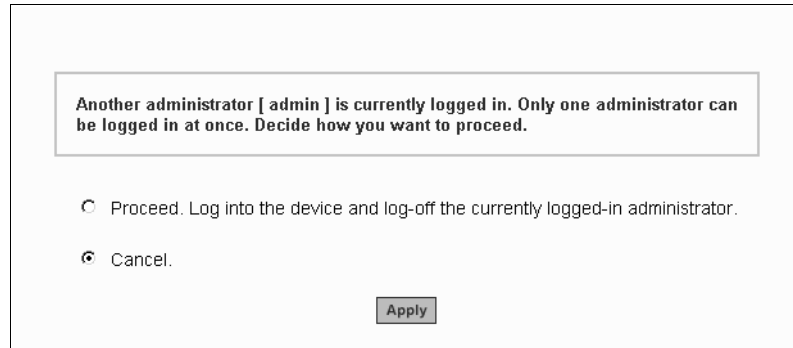
Table 1-4: User Types, Responsibilities, and Default Password

User Name	Responsibilities	Default Password
root	Cannot be deleted. Only console logins allowed. Runs the <code>wiz</code> command to do initial network configuration, as described in “Configuring Basic Networking Using the <code>wiz</code> Command” on page 77. Access Privileges: Full Read/Write/Delete.	cyclades
admin	Cannot be deleted. Has all access: through the Web Manager in Wizard and Expert mode, and through the OSD. Has full access to every function of the Web Manager. Access Privileges: Full Read/Write/Delete.	cyclades
<i>administratively-assigned</i>	User account configured by the administrator to be able to administer devices connected to the ports of the KVM/net. Has access to the port through the Web Manager and through the OSD. Regular users can access and administer only devices that are connected to ports to which they are assigned. Default Access Privileges for generic users: Read/Write only for all ports. Administrators can restrict access for individual users to Read only to specific ports. If an administrator assigns a regular user to the “admin” group, that user can also perform the same administrative functions on the Web Manager as the “admin” user, as described above.	<i>administratively-assigned</i>

Simultaneous KVM/net Logins

Only one KVM/net administrator can be logged in at a time. If a second administrative user attempts to log into the Web Manager, the following

prompt appears offering a choice of cancelling the attempt to log in or terminating the other administrator's login session.



Another administrator [admin] is currently logged in. Only one administrator can be logged in at once. Decide how you want to proceed.

Proceed. Log into the device and log-off the currently logged-in administrator.

Cancel.

Apply

Simultaneous Server Connections

The KVM/net supports a maximum of 5 concurrent server connections. Up to two local connections are supported. One connection can be a remote KVM connection over the Ethernet. And up to ? connections can be inband depending on whether a KVM connection is being made. The types of user connections that can be made are explained below:

- Local users include:
 - One local user at the KVM/net (User 1).
 - One extended user at the AlterPath KVM RP location (User 2).
- IP users include:
 - KVM – The KVM/net supports one KVM over IP connection
 - in-band – KVM/net supports up to four concurrent in-band connections depending on the number of KVM connections being made. Since the maximum total IP connections is four, if one KVM connection is being made, only three in-band connections can be made at that time.

The following table lists the number and types of server connections that can be made over IP based on the number of local users connected to KVM ports.

Table 1-5: Number of Simultaneous Server Connections

Users	No Local Users	One Local User	Two Local Users
KVM over IP	1	1	-
Inband	4	3	4
Total	5	6	6

Administration Options

The following sections summarize the KVM/net administration options:

- “Cyclades Web Manager” on page 20
- “On-Screen Display” on page 20
- “Linux Commands and KVM/net-specific Commands” on page 21

The administrator options require different types of log in credentials. For more information on which types of users can perform administrative tasks and access administrative options, see “Cyclades Web Manager” on page 21.

Table 1-6: Administration Options

Cyclades Web Manager	<p>The Web Manager is the primary means of configuring the KVM/net and administering its connected devices.</p> <ul style="list-style-type: none">• See “Prerequisites for Using the Web Manager” on page 22 for an introduction that includes prerequisites for using the Web Manager and explanations about how the different types of user accounts use the Web Manager.• See “Web Manager for Administrators” on page 123 for more details about how KVM/net administrators use the Web Manager.
On-Screen Display	<p>The on-screen display (OSD) can be used locally from a keyboard, monitor and mouse that is directly-connected to the KVM/net. When the monitor and the KVM/net are on, the OSD login screen appears on the monitor.</p> <ul style="list-style-type: none">• See “To Connect to the User 1 Management Port” on page 75 for how to make the hardware connection.• See “On Screen Display” on page 317 for how KVM/net administrators and administrators of connected devices use the OSD.

Table 1-6: Administration Options (Continued)

Linux Commands and KVM/net- specific Commands	<p>The KVM/net offer the following types of access allowing administrators to log in and enter Linux commands and KVM/net-specific commands in a shell running on the KVM/net:</p> <ul style="list-style-type: none"> • A local administrator who has a direct connection to the console port on the KVM/net, who is running a terminal or terminal emulation program, and who knows the root password. The direct login requires authentication using the root password. The default shell defined for the root user is bash. • A remote administrator who uses telnet or ssh to connect to the KVM/net and log in as root. <p>See “To Connect to the Console Port” on page 74, “To Dial Into the KVM/net Plus Using a Terminal Emulator” on page 346, and “Configuring Basic Networking Using the wiz Command” on page 77.</p>
--	--

Cyclades Web Manager

Administrators perform most tasks through the KVM/net’s version of the Cyclades Web Manager. The Web Manager runs in a browser and provides a real-time view of all the equipment that is connected to the KVM/net. The administrator or the regular user who has administrative access can use the Web Manager to configure users and ports, troubleshoot, maintain, cycle power, and reboot the connected devices, either while on site or from a remote location. KVM/net also allows regular users and administrators to use the Web Manager to access devices that are connected to KVM ports.

Web Manager uses forms and dialog boxes (which are pop-up windows) to receive data input. See also, “Prerequisites for Using the Web Manager” on page 22.

Administrators see “Web Manager for Administrators” on page 123. Operators, see “Web Manager for Regular Users” on page 267.

Prerequisites for Using the Web Manager

The prerequisites described in this section must be complete before anyone can access the Web Manager. If you have questions about any of the following prerequisites, contact your site's system or network administrator.

- An administrator needs to define basic network parameters on the KVM/net so the Web Manager can be launched over the network.

See "Configuring Basic Networking Using the wiz Command" on page 77 for how to define network parameters on the KVM/net.

The administrator also needs the following to be able to connect to the KVM/net through the Web Manager:

- A networked Windows computer that has access to the network where the KVM/net is installed.
- A supported browser (see Table 1-7).

Table 1-7: Supported Browsers

Internet Explore 5, 6

Netscape 7

Mozilla

Firefox

- The IP address of the KVM/net.
Entering the IP address of the KVM/net in the address field of one of the supported browsers listed in Table 1-7 is the first step required to access the Web Manager.

When DHCP is enabled, a device's IP address may change each time the KVM/net is booted up. Anyone wanting to access the KVM/net must find out the currently-assigned IP address. If DHCP is enabled and you do not know how to find out the current IP address of the KVM/net, contact your system administrator for help. For more information, see "Considerations When Choosing Whether to Enable DHCP" on page 50.

- A user account defined on the Web Manager
By default, the admin has an account on the Web Manager. An administrator can add regular user accounts to administer connected devices using the Web Manager.

TCP Ports

The TCP port numbers for KVM ports are used by the AlterPath Viewer when a user connects to a KVM port through the Web ManagerKVM/net. When a user connects to a KVM port through the Web Manager, the AlterPath Viewer uses port 5900. If a second IP module exists, port 5901 is used for the second AlterPath Viewer launched over IP. You can assign a different port number or numbers through the OSD or the Web Manager. Do not assign reserved TCP port numbers 1 through 1024.

Special circumstances may require KVM/net administrators to specify alternative TCP port numbers other than the defaults. For example, the firewall may block TCP port 5900 or 5901.

The following table provides links to procedures for changing default TCP port numbers and port aliases.

Table 1-8: Tasks: Configuring TCP Port Numbers and Port Aliases

Task	Where Described
Change the TCP port number(s) assigned to the AlterPath Viewer(s)	“To Assign Alternate TCP Port Numbers for the AlterPath Viewer” on page 130
Assign an alias describing the connected server to the KVM port	“To Configure an Alias for a KVM Port” on page 227
Change the TCP port number(s) assigned to in-band connections	“To Add or Modify an In-band (RDP) Server” on page 199

Cascaded Devices

The KVM/net supports cascading, which allows administrators to connect secondary KVM units to a primary KVM/net. Cascading allows administrators to increase the number of managed devices to up to 1024 servers with a centralized configuration and access interface.

The following diagram depicts a basic cascaded configuration of a primary KVM/net with 32 ports and one KVM and one KVM Expander cascaded from it.

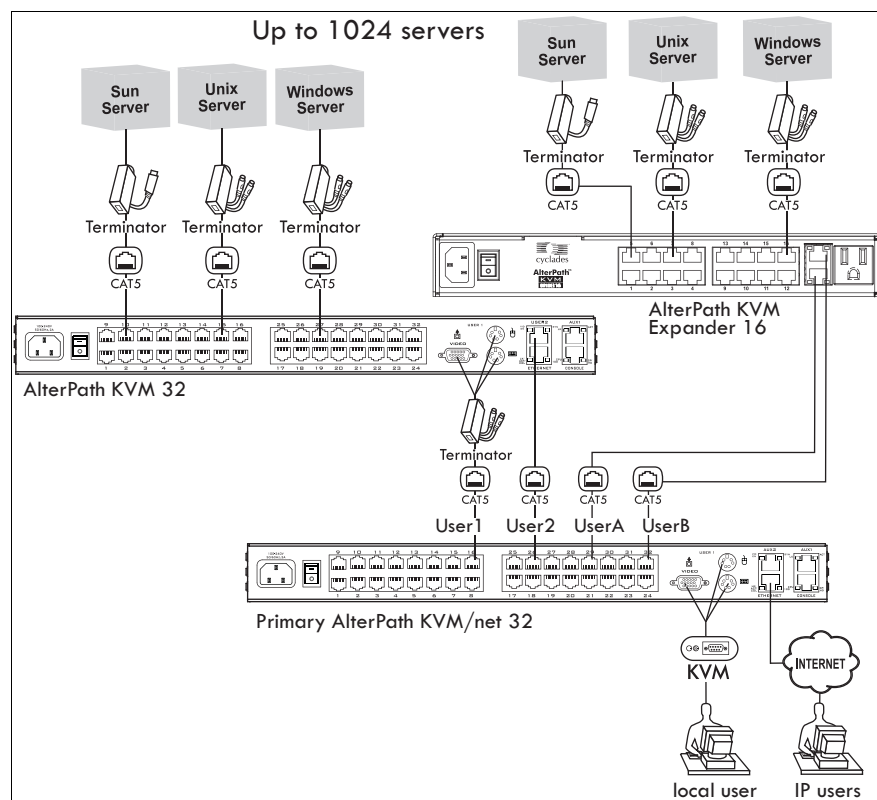


Figure 1-9: Cascaded KVM Devices from an KVM/net

As depicted in the previous figure, the KVM/net support one level of cascading: The primary KVM/net controls the secondary level of KVM units connected to it. A secondary KVM unit can be a KVM or a KVM Expander.

Administrators can connect up to 32 KVM units to the master KVM/net. Each cascaded KVM device has two management ports that can be connected to the primary KVM/net. You can connect any one of the master KVM/net's KVM ports to either the User 1 or User 2 management ports on the cascaded KVM or to the User A or User B management ports on the KVM Expander. The following table indicates which ports on each cascaded device can be used for cascading and which cables need to be used in order to connect them.

Table 1-9: Connectors and Ports for Cascading KVM Units

KVM Unit	Management Ports	Connectors
KVM Expander	User A, User B	CAT5 cable
KVM	User 1, User 2	CAT5 cable KVM Terminator (User1)
AlterPath KVM/net	User 1, User 2	CAT5 cable KVM Terminator (User1)
KVM/net Plus	User 1, User 2	CAT5 cable KVM Terminator (User1)

Note: In addition to a CAT5 cable, you need a KVM Terminator to connect to the User 1 port of a cascaded KVM/net Plus, KVM/net, or KVM.

KVM/net users can use the master KVM/net to access all devices connected to KVM ports on the master and primary KVM units.

KVM/net Port Permissions

In the default configuration, no users except “admin” and “root” can access any ports. The KVM/net administrator configures access for regular users as desired.

The following table summarizes the default port access permissions and default authentication types (Auth Type) and provides links to where the port permissions are described in more detail.

Table 1-10:Default Port Access Permissions

Default Access	Default Auth Type	Access Types	Where Documented
None	Local	No access Read only Read/Write Full access (Read/Write/Power management)	“Understanding KVM Port Permissions” on page 27 “To Assign KVM Port Access to a User or Group” on page 180

The KVM/net administrator must take the actions described under “Where Documented” to allow any other types of access than the defaults defined in the previous table. See “Authentication” on page 44 for the tasks related to setting up authentication.

Understanding KVM Port Permissions

KVM port permissions are defined in the Web Manager by assigning *Default Permissions* that apply to all KVM ports and by optionally assigning specific permissions to individual ports or groups of ports. The options for “Default Permissions” are shown in the following list.

- No access [Default]
- Read only
- Read/Write
- Full access (Read/Write/Power management)

For individual users and groups, if desired, the KVM/net administrator can construct lists of KVM ports with the following types of permissions:

- Ports with no permission
- Ports with read only permission
- Ports with read/write permission
- Ports with full permission

A *Generic User* account has a default set of permissions that apply to all regular users and groups. The Generic User’s Default Permission is “No access.”

To allow users to access KVM ports, the KVM/net administrator must do one or both of the following:

- Change the permissions assigned to the Generic User
- Change the permissions assigned to individual users or to groups of users

Editing the Generic User allows you to change the KVM port permissions for all regular users and groups at once.

The KVM/net administrator can specify different Default Permissions or KVM port permissions for any user or group. “KVM Port Permissions Hierarchy” on page 28 provides information that the KVM/net administrator needs to understand in order to perform advanced configuration of KVM permissions.

The following table shows the tools that the KVM/net administrator can use to set KVM port permissions and where in this manual to go for further details.

Table 1-11:Tools for Setting KVM Port Permissions

Tools	Where Documented
Web Manager	“To Assign KVM Port Access to a User or Group” on page 180
OSD	“KVM Ports Screens” on page 358

KVM Port Permissions Hierarchy

If you specify individual KVM port permissions or default permissions for users and groups, you need to understand the following information about how the system handles requests from a user who is trying to access a KVM port. The following series of decisions is made.

Decision 1: Check User’s KVM Port Permissions

1. Does the user have specific KVM port permissions that allow or deny access to the port?
 - If yes, access is allowed or denied.
 - If no, go to Decision 2.

Example for Decision 1

- If user john is trying to access KVM port 4 and his account has port 4 in a list of ports with full permission, then john is given read/write and power management access.
- If user jane is trying to access port 4 and her account has port 4 in a list of ports with no permission, then jane is denied access.
- If users jim, joan, jerry, jill, joe, jennifer, jordan, jolanda, and jezebel are trying to access port 4 and do not have port 4 listed for any types of access, then their access requests are passed to decision 2.

Decision 2: Check Group's KVM Port Permissions

2. Is the user included in a group with KVM port permissions that allow or deny access to the port?
 - If yes, access is allowed or denied.
 - If no, skip to Decision 3.

Note: When a user is in more than one group, the most restrictive permission is used.

Example for Decision 2

- If user jim is trying to access port 4 and he is a member of a group called linux_ca2 that has port 4 in a list of ports with read/write permissions, then jim is given read/write access.
- If user joan is trying to access port 4 and she is in a group called linux_ca3 that has port 4 in a list of ports with no permission, then joan is denied access.
- If jerry and jill are trying to access port 4 and are in a group called linux_ca4 that has no specific port permissions defined, then their access requests are passed to decision 3.
- If joe, jennifer, jordan, jolanda, and jezebel are trying to access port 4 and are not in any group, then their access requests are passed to decision 3.

Decision 3: Check Generic User's KVM Port Permissions

3. Does the Generic User have specific KVM port permissions that allow or deny access the port?
 - If yes, access is allowed or denied.
 - If no, go to decision 4.

Example for Decision 3

- If user jerry is trying to access port 4 and the Generic User has port 4 in a list of ports with full access permissions, then jerry is given read writer and power management access.

- If user jill is trying to access port 4 and the Generic User has port 4 in a list of ports with no access permissions, then jill is denied access.
- If users joe, jennifer, jordan, jolanda, and jezebel are trying to access port 4 and the Generic User does not have port 4 listed for any type of access, then their access request are passed to decision 4.

Decision 4: Check User's Default Permissions

4. Does the user have a Default Permission that allows or denies access to the port?
 - If yes, access is allowed or denied.
 - If the user has no Default Permission, the user is under the Generic User's default permission, and the request for access goes to decision 5.

Example for Decision 4

- If user joe is trying to access port 4 and he has a Default Permission that allows read only access to ports, then joe is given read only access.
- If user jennifer is trying to access port 4 and she has a Default Permission that allows no access to ports, then jennifer is denied access.
- If users jordan, jolanda, and jezebel are trying to access port 4 and their Default Permissions are under the Generic User's Default Permission, then their access requests are passed to decision 5.

Decision 5: Check Group's Default Permissions

5. Does the user belong to a group that has a Default Permission that allows or denies access to the port?
 - If yes, permission is granted or denied.
 - If no, go to decision 6.

Example for Decision 4

- If user jordan trying to access port 4 is in a group called windows_ca1 that has a Default Permission of full, then jordan is given read/write and power management access.
- If user jolanda trying to access port 4 is in a group called windows_ca2 that has a Default Permission of no access, then jolanda is denied access.

- If user jennifer is not a member of any group with a Default Permission specified, then her access request is passed to decision 6.

Decision 6: Check Generic User’s Default Permissions

Note: If an access request gets this far, the Default Permission of the Generic User is the only permission that could apply.

6. Does the Default Permission for the Generic User allow access to the port?
- If yes, access is granted.
 - If no, access is denied.

Server Access: In-band and Out of Band

KVM/net users can access servers over the Ethernet using the following methods:

- In-band access – An IP address is used to connect to and control Windows (Win2000, 2003, XP, and NT) Terminal Servers.
- Out-of-band access – KVM ports are used to connect to and control USB Sun servers running Solaris or PCs running a Windows, Linux, or other open source operating system.

The differences between the in-band and out-of-band connection methods are briefly described in the following table. For a more detailed description of the requirements and functionality of each connection method, see the following section, “Determining the Connection Type and its Supported Functionality” on page 33

	In-band	Out-of-Band
Connection Type	Remote Desktop Protocol (RDP) over the Ethernet or PPP	Keyboard, video, mouse (KVM) CAT5 connection to a KVM/net and Ethernet or PPP access to the KVM/net Web Manager

	In-band	Out-of-Band
Supported Source Computers	Client machine running a Windows operating system with a valid IP address	All Windows clients
Supported Target Servers	Windows (Win2000, 2003, XP, and NT) Terminal Servers	USB Sun servers running Solaris or PCs running a Windows, Linux, or other open source operating system
Supported Browsers	Internet Explorer 5, 6	Internet Explorer 6, Netscape 7, Mozilla, Firefox
Direct Log In	Not available	Available if configured by the KVM/net administrator See “To Enable Direct Access to KVM Ports [Expert]” on page 156
Power Management While Connected	Not available	Available if configured by the KVM/net administrator and if the server is plugged into an AlterPath PM IPDU that is connected to the KVM/net. See “Power Management” on page 41
Viewer	ActiveX viewer See “Viewing In-band Connections” on page 280	AlterPath Viewer See “Viewing KVM Connections” on page 278

Determining the Connection Type and its Supported Functionality

When a user wants to connect to a server displayed on the Web Manager Connect to Server form, the drop-down list indicates whether the server can be accessed by a KVM connection, an in-band connection, or both. In the connect list, all servers connected to KVM ports appear first followed by all servers that are accessed through in-band connections and are not connected to KVM ports; those servers that can be connected by both methods appear at the bottom of the list.

The types of connections that can be made to each server is displayed in parenthesis at the end of each server entry in the list. The following table describes the functionality of each connection type.

Table 1-12: Available Functionality During KVM and In-band Connections

Server Connection Labels	Description
(KVM)	<p>Indicates that the server can be accessed only through an out-of-band, KVM connection.</p> <p>This server is connected to a KVM port on the KVM/net or on a cascaded KVM unit.</p> <p>Users can control all applications on the server, have BIOS access, and can view POST, and boot messages. Users can access this server even when the network is down or after a system boot is completed.</p> <p>Users can also control the power flow on this server if the server is plugged into an AlterPath PM IPDU and the port is properly configured for power management.</p>
(Inband)	<p>Indicates that the Microsoft Terminal Server running RDP can be accessed only through an in-band connection and is not connected to a KVM port.</p> <p>Users can access this server only to run applications once the server is already running. The performance on in-band connections is slightly better than that of KVM connections and no synchronization of keyboard and mouse is necessary.</p>

Table 1-12: Available Functionality During KVM and In-band Connections (Continued)

Server Connection Labels	Description
(KVM + Inband)	<p>Indicates that the server can be accessed through in-band and out-of-band (KVM) connections.</p> <p>The first time users select this server from the Connect drop-down list, an in-band connection is attempted. The connection automatically switches to KVM only if the in-band connection fails or if an in-band connection to this server already exists. Users who want to access this server with a KVM connection, must do one of the following:</p> <ul style="list-style-type: none"> • Make two connection attempts to the same server from the Web Manager Connect to Server form. <p>The first connection is an in-band connection viewed through an ActiveX viewer. The second connection is a KVM connection viewed through the AlterPath Viewer.</p> <p>See “To Connect to Servers Through The Web Manager’s Connect To Server Form” on page 290.</p> • Make a direct login to the KVM port. <p>See “Login Screen: Direct Logins Enabled, Only IP Address Entered” on page 284 and “Login Screen: Direct Logins Enabled, IP Address and Port Entered” on page 284 for more information.</p>

Administering Users of Connected Servers

This section reviews the tasks that KVM/net administrators need to do to enable access to connected servers.

The “admin” account can add new regular user accounts to allow others to connect to ports and administer or use connected devices.

Types of Access to Ports

The KVM/net administrator can restrict regular user accounts to allow them to only manage specific servers and devices. Each account can have one of the following types of access after login:

- Read only
- Read write
- Read write power

Note: The KVM/net offers access privileges to KVM ports only. In-band connections are authenticated, and the access privileges are granted on the in-band server itself.

Tasks Related to Access to Connected Devices

Planning should include the following steps:

- Create a list of servers to connect to the KVM/net.
- Decide whether the servers need to be connected to ports for KVM access, need to have RDP enabled for in-band access, or both.
- Create a list of user accounts with the type of access each user needs to which ports.
- Obtain usernames and passwords with the proper permissions for connected servers to give to the KVM/net users who will connect to these servers.
- Create meaningful aliases to assign to port numbers and in-band Windows Terminal Servers.
- List all the devices that need to be connected to IPDUs and the users who can access them.

Introduction

During setup of the KVM/net, the installer connects the desired servers to the ports as planned.

During configuration, the KVM/net administrator does the following, if desired:

- Assigns aliases to ports to identify the connected servers.
- Assigns aliases to IPDUs to identify the location or types of devices being managed.
- Creates accounts for users of connected devices.
- Specifies which ports each user can access and which type of access each can have.
- Specifies an authentication method for access to the KVM/net and to all KVM ports.
- Redefines keyboard shortcuts (hot keys) if desired.
- Redefines TCP port numbers used for accessing KVM ports, if desired.

See the following table for a list of related tasks and where they are documented.

Task	Where documented
Specify an alias for a KVM port.	<ul style="list-style-type: none">• “To Specify or Change the Alias for a KVM Port” on page 174
Specify an alias for a PM.	<ul style="list-style-type: none">•
Assign permissions to access ports.	<ul style="list-style-type: none">• “To Assign KVM Port Access to a User or Group” on page 180
Assign permissions to IPDUs and outlets.	<ul style="list-style-type: none">• “To Configure Users to Manage Specific Power Outlets” on page 148

Redefining Keyboard Shortcuts (Hot Keys)

Predefined keyboard shortcuts (also called hot keys) allow users to do the following:

- Perform common actions while connected through a KVM port
- Emulate Sun keyboard keys while connected through a KVM port to a Sun server.

If desired, the KVM/net administrator can redefine the default hot keys either through the Web Manager or the OSD.

Redefining KVM Connection Hot Keys

The hot key sequences used while connected to KVM ports have two parts, which are called the *common escape sequence* and the *command key*. The default common escape sequence is `Ctrl+k`, and the command key is different for each command. For example, the `q` command key is entered after `Ctrl+k` to quit the login session as shown here: `Ctrl+k q`. See “Hot Keys for KVM Connections” on page 295 for the defaults. Under `Configure>KVM` in the Web Manager, the common escape sequence is defined separately from the command keys. KVM/net administrators can redefine two different sets of command keys for users accessing KVM ports through the OSD through the User 1 or User 2 connection and through the Web Manager.

Redefining Sun Keyboard Equivalent Hot Keys

The KVM/net provides a default set of hot keys for use while connected to Sun servers through KVM ports to emulate keys that are present on Sun keyboards but are not present on Windows keyboards. The hot keys are made up of an escape key followed by a function key. See “Hot Keys for Emulating Sun Keyboard Keys” on page 296 for more details. The default escape key is the Windows key, which is labeled with the Windows logo. KVM/net administrators can redefine the Sun emulation escape key to be one of the following: Ctrl, Shift, or Alt.

Summary of Tasks for Redefining Hot Keys

See the following table for a summary of tasks for redefining keyboard shortcuts with references to where they are documented.

Table 1-13:Tasks for Redefining Hot Keys

Part	Web Manager Form	Where Documented	OSD Form	Where Documented
KVM Common escape sequence	Configuration>KVM>General>General	“To Redefine KVM Session Keyboard Shortcuts [Expert]” on page 157	Configure>General	“General Configuration Screens [OSD]” on page 386
KVM Command keys for the local user session	Configuration>KVM>General>User 1 Configuration>KVM>General>User 2	“To Redefine KVM Session Keyboard Shortcuts [Expert]” on page 157	Configure>User Station	“User Station Screens” on page 414
KVM Command keys for IP user sessions	Configuration>KVM>General>IP Users		N/A	
Sun keyboard emulation escape key	Configuration>KVM>General	“To Redefine the Escape Key for Sun Keyboard Emulation Hot Keys [Expert]” on page 236.	Configure>General	“KVM Ports Screens” on page 417

Packet Filtering on the KVM/net

IP filtering refers to the selective blocking of the IP packets based on certain characteristics. The KVM/net can be configured to filter packets like a firewall.

The IP Filtering form is structured in two levels:

- Chain – The IP Filtering form which contains a list of chains
- Rule – The chains which contain the rules that control filtering

IP filtering refers to the selective blocking of the passage of IP packets between global and local networks. The filtering is based on rules that describe the characteristics of the packet (that is, the contents of the IP header, the input/output interface, or the protocol).

This feature is used mainly in firewall applications to filter the packets that could potentially crack the network system or generate unnecessary traffic in the network.

The following table describes the different levels of IP filtering

Table 1-14:Levels of IP Filtering

Chain	<p>The filter table contains a number of built-in chains and may include user-defined chains. The built-in chains are called according to the type of packet. User-defined chains are called when a rule which is matched by the packet points to the chain. Each table has a set of built-in chains classified as follows:</p> <ul style="list-style-type: none"> • INPUT - For packets coming into the box itself. • FORWARD - For packets being routed through the box. • OUTPUT - For locally-generated packets.
--------------	---

Table 1-14:Levels of IP Filtering (Continued)

Rule	<p>Each chain contains a sequence of rules that control filtering. The rules address the following issues:</p> <ul style="list-style-type: none">• How the packet should appear in order to match the rule <p>Some information about the packet is checked according to the rule, for example, the IP header, the input and output interfaces, the TCP flags and the protocol.</p> <ul style="list-style-type: none">• What to do when the packet matches the rule <p>The packet can be accepted, blocked, logged, or jumped to a user-defined chain.</p> <p>When a chain is analyzed, the rules of this chain are reviewed one-by-one until the packet matches one rule. If no rule is found, the default action for that chain will be taken.</p>
-------------	---

Power Management

The KVM/net enables users who have power management permissions to power off, power on, and reboot remote devices connected to an AlterPath PM intelligent power distribution unit (IPDU). By connecting one PM to the AUX port and by daisy-chaining any combination of PM models, you can connect up to 128 outlets to one KVM/net.

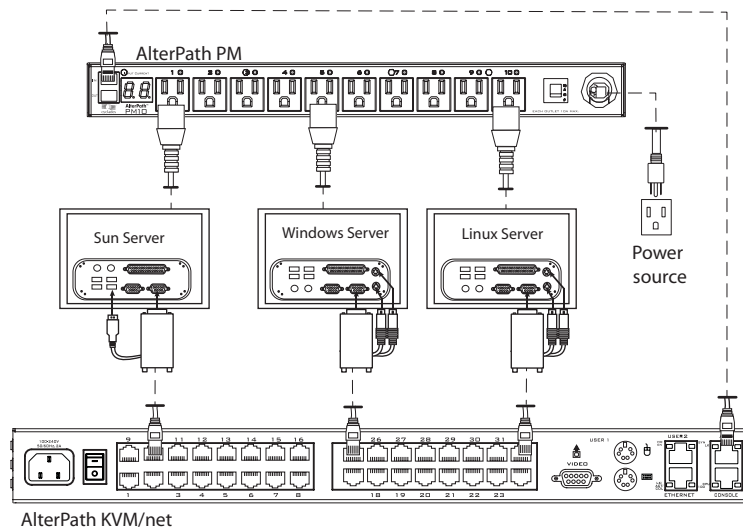


Figure 1-10:Connecting an AlterPath PM to the KVM/net

See “Setting Up and Configuring Power Management” on page 42 for information about the procedures the KVM/net administrator must perform before anyone can use the tools to manage power.

KVM/net users most commonly perform power management through the Web Manager. See “Options for Managing Power” on page 43 for more information.

Setting Up and Configuring Power Management

Administrators most commonly assign power management permissions to users and configure ports for power management using the Web Manager. However, the OSD also offers menus for configuring power management on local devices.

Two types of power management can be set up and configured on the KVM/net:

- Power management of any device plugged into an IPDU connected to the AUX port.
See “Controlling Power Through the Web Manager IPDU Power Management Forms” on page 43.
- Power management while accessing a server connected to a KVM port and plugged into an IPDU connected to the AUX port.
See “Controlling Power While Connected to KVM Ports” on page 44

The following set up and configuration tasks must be performed for both types of power management:

Task	Where Documented/Notes
1 Install PM units.	<ul style="list-style-type: none">• “To Connect a PM to the AUX Port” on page 106• “To Connect Multiple PMs to the KVM/net” on page 107
2 Configure the AUX port for use with power management.	“To Configure the AUX Port for Use With a PM or an External Modem” on page 240
3 Plug devices into outlets on the PM connected to the AUX port.	This allows users to control power of the plugged devices from the Web Manager Access page. Refer to the documentation of your PM model for more information if needed.
4 Configure users to manage power.	“To Configure Users to Manage Specific Power Outlets” on page 148

The following additional configuration tasks must be performed for power management while accessing a server connected to a KVM port and plugged into an IPDU connected to the AUX port:

Task	Where Documented/Notes
5 Plug servers connected to KVM ports into outlets on the PM connected to the AUX port.	This is the first step in allowing users to control power not only from the Web Manager Access page, but while connected to KVM ports as well. Refer to the documentation of your PM model for more information if needed.
5 Associate the ports to which the servers are connected with the power outlets to which the servers are plugged in.	“To Configure a KVM Port for Power Management [Expert]” on page 165
6 Give users full access (read, write, power) permission on the KVM port(s).	“To Assign KVM Port Access to a User or Group” on page 180

Options for Managing Power

The sections listed below describe the different ways that users with power management permissions (called authorized users) can perform power management through the KVM/net and provide links to related information and procedures.

The following sections describe the different ways authorized users can manage power on connected devices.

Controlling Power Through the Web Manager IPDU Power Management Forms

Through the Web Manager’s IPDU Power Management form, users with power management permissions can perform power management on any device plugged into a PM connected to the AUX port. See “Power Management for Regular Users” on page 273.

Administrators must configure users for IPDU power management. See “To Configure Users to Manage Specific Power Outlets” on page 148. Or see “Setting Up and Configuring Power Management” on page 42 for a list of all of the administration tasks involved in setting up power management.

Controlling Power While Connected to KVM Ports

Users who have power management permissions can do power management while connected to servers through KVM ports by using a keyboard shortcut that brings up a power management screen. The default keyboard shortcut is Ctrl+k p.

The following table lists the power management options for authorized users, the KVM/net interface(s) used for each option, and where each option is documented.

Administrators must perform multiple configuration tasks in order to set up and grant users permission for power management. See “Setting Up and Configuring Power Management” on page 42 for a list of all of the administration tasks involved in setting up power management.

Security

The KVM/net comes with the following configurable security features:

- Encryption
See Encryption.
- Authentication
See Authentication.

Encryption

Administrators can specify that communications are encrypted between the KVM/net and any computer attached to a KVM port. In the Web Manager, the administrator chooses Expert>Configuration>KVM>Security to bring up the IP security form.

See “Security” on page 183 for instructions.

Authentication

Anyone accessing the KVM/net must log in by entering a username and password. Controlling access by requiring users to enter names and passwords is called authentication. Usernames and passwords entered during login attempts are checked against a database that lists all the valid usernames along

with the encrypted passwords. Access is denied if the username or password is not valid. The password database that is used for checking can reside either locally (on the KVM/net) or on an authentication server on the network. The selected authentication server must be already installed and configured in order for authentication to work. Using one or more of the many types of popular authentication methods supported on the KVM/net can reduce administrator workload when a user account needs to be added, modified, or deleted.

Choosing Among Authentication Methods

The administrator can select among authentication methods to control logins to the following components:

- For logins to the KVM/net
The authentication method chosen for the KVM/net is used for subsequent access through `telnet`, `ssh`, or the Web Manager.
- For logins to all KVM ports

The following table describes the supported authentication methods and indicates which methods are available for the KVM/net and which are available for KVM ports. All authentication methods except “Local” require an authentication server, which the administrator specifies while selecting the authentication method. The KVM/net uses local authentication if any of the authentication servers fails.

Table 1-15:Supported Authentication Types for KVM/net and Port Types

Authentication Type	Description	KVM/net	All KVM Ports
None	No login required	N/A	X
Local	Uses user/password file for local authentication on the KVM/net	X [Default]	X [Default]
Kerberos	Uses Kerberos network authentication protocol	X	X
Kerberos/Local	Uses local authentication if Kerberos authentication fails	X	X

Table 1-15:Supported Authentication Types for KVM/net and Port Types (Continued)

Authentication Type	Description	KVM/net	All KVM Ports
KerberosDownlocal	Uses local authentication if Kerberos server is down	X	X
LDAP	Uses LDAP (Light-weight directory access protocol)	X	X
LDAP/Local	Uses local authentication if LDAP authentication fails	X	X
LDAPDownlocal	Uses local authentication if LDAP server is down	X	X
NIS	Uses NIS authentication	X	X
NIS/Local	Uses local authentication if NIS authentication fails	X	X
NISDownlocal	Uses local authentication if NIS server is down	X	X
NTLM	Uses SMB authentication for Microsoft Windows NT/2000/2003	N/A	X
RADIUS	Uses RADIUS authentication	X	X
RADIUSDownlocal	Uses local authentication if RADIUS server is down	X	X

Table 1-15:Supported Authentication Types for KVM/net and Port Types (Continued)

Authentication Type	Description	KVM/net	All KVM Ports
RADIUS/local	Uses local authentication if RADIUS authentication fails	X	X
TACACS+	Uses Terminal Access Controller Access Control System (TACACS+) authentication.	X	X
TACACS+/Local	Uses local authentication if TACACS+ authentication fails	X	X
TACACS+Downlocal	Uses local authentication if TACACS+ server is down	X	X

Tools for Specifying Authentication Methods

The administrator generally uses the Web Manager for specifying an authentication method for the KVM/net and for all KVM ports, as described in “Configuring an Authentication Method” on page 185. Optionally, the administrator can use the OSD (on screen display) for selecting an authentication method and specifying an authentication server (when needed).

The following table lists the tasks necessary for specifying authentication methods using the Web Manager and the OSD:

Table 1-16:Specifying Authentication Methods

Task	Where Documented/Notes
Choosing an authentication method for the KVM/net	<ul style="list-style-type: none"> • Web Manager – “To Configure an Authentication Method for KVM/net Logins” on page 186 • OSD – “Authentication Screens” on page 374

Table 1-16: Specifying Authentication Methods (Continued)

Task	Where Documented/Notes
Choosing an authentication method for the for all KVM ports	<ul style="list-style-type: none"> • Web Manager – “To Configure an Authentication Method for Logins Through KVM Ports” on page 187 • OSD – “General Configuration Screens [OSD]” on page 327
Configuring a remote authentication server	<p>If configuring any authentication method other than Local, an authentication server must be set up for that method.</p> <ul style="list-style-type: none"> • Web Manager – “Configuring Authentication Servers for Logins to the KVM/net and Connected Devices” on page 188 • OSD – “Authentication Screens” on page 374

Notifications, Alarms, and Data Buffering

The KVM/net administrator can set up logging, notifications, and alarms to alert remote administrators about problems. System-generated messages about the KVM/net, any connected IPDUs, computers, or other devices can be sent to syslog servers for handling.

The KVM/net administrator can also set up data buffering, so that data from communications with KVM-connected computers can be stored in files at the following locations:

- Local —stored in the KVM/net flash memory
- Remote files—stored in either of the two following types of servers:
 - NFS servers
 - Syslog servers

For more details about syslog servers see, “Syslog Servers” on page 49.

For more background about setting up logging, notifications, alarms, and for links to all related procedures in this manual, see “Configuring Logging and Alarms” on page 50.

Syslog Servers

Messages about the KVM/net, its connected IPDUs, and other connected devices can be sent to central logging servers, called syslog servers. Data from KVM-connected computers can optionally be stored in files on syslog servers.

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

Prerequisites for Logging to Syslog Servers

An already-configured syslog server must have a public IP address that is accessible from the KVM/net. The KVM/net administrator must be able to obtain the following information from the syslog server's administrator.

- The IP address of the syslog server
- The facility number for messages coming from the KVM/net.

Facility numbers are used on the syslog server for handling messages generated by multiple devices. See “Facility Numbers for Syslog Messages” on page 49 for more background on how facility numbers are used.

Facility Numbers for Syslog Messages

Each syslog server has seven local facility numbers available for its system administrator to assign to different devices or groups of devices at different locations. The available facility numbers are: Local 0 through Local 7.

Example of Using Facility Numbers

The syslog system administrator sets up a server called “syslogger” to handle log messages from two KVM/nets. One KVM/net is located in São Paulo, Brazil, and the other KVM/net is in Fremont, California. The syslog server's administrator wants to aggregate messages from the São Paulo KVM/net into the `local1` facility, and to aggregate messages from Fremont KVM/net into the `local2` facility.

On “syslogger” the system administrator has configured the system logging utility to write messages from the `local1` facility to the `/var/log/saopaulo-config` file and the messages from the `local2` facility to the `/var/log/fremont-config` file. While identifying the syslog server using

the Web Manager, according to this example, you would select the facility number Local 2 from the Facility Number pull-down menu on the System Logger form.

Configuring Logging and Alarms

The following procedures configure logging, alarms, and data buffering.

- “To Add a Syslog Server [Wizard]” on page 140
- “To Delete a Syslog Server [Wizard]” on page 140
- “To Configure Syslogging for KVM Ports and Specify Message Filtering [Expert]” on page 208
- “To Configure Creation of Alarms and Syslog Files for IPDUs [Expert]” on page 150

Considerations When Choosing Whether to Enable DHCP

DHCP is enabled by default. It relies on a DHCP server known to the KVM/net. Because a DHCP server may assign a different IP address every time the KVM/net reboots, when DHCP is enabled, a user needs to take an additional step to find out the dynamically-assigned IP address before being able to bring up the Web Manager. Following are three ways to find out the dynamically-assigned IP address:

- Make an inquiry to the DHCP server on the network where the KVM/net resides, using the MAC address (a 12-digit hexadecimal number, which is on a label at the bottom of the KVM/net).
- Connect to the KVM/net remotely using `telnet` or `ssh`.
- Connect directly to the KVM/net to find out the DHCP address using the `ifconfig` command.

KVM Terminator Usage and Types

An AlterPath KVM terminator is used when connecting a computer or a cascaded KVM device to a KVM port on the AlterPath KVM/net.

Administrators or operators at remote stations who have access through the KVM/net's management software to a KVM port have the same kind of access as if they were using the actual keyboard, mouse, and monitor of the computer that is connected to the port.

The terminator comes in three models shown in the following table

Table 1-17:AlterPath KVM Terminators

Server Type	Connection	KVM Terminator Model	Part Number
PC	Mini DIN 6-pin (COM)	PS/2	ATP4610
PC	USB port	PC USB	ATP4620
USB Sun	USB port. (This terminator does not work with all Sun computers. The Sun computer must have a VGA and USB port.)	Sun USB	ATP4630

See “To Connect Computers to KVM Ports” on page 72 for instruction on using the KVM Terminators.

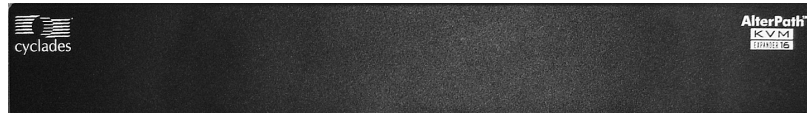
When a KVM/net is ordered, the customer selects a KVM terminator for each type of computer to be connected to the KVM/net's KVM ports. For example, when ordering a KVM/net with four KVM ports to be connected to two Windows servers with DIN connectors and two Sun servers with VGA ports and USB connectors, the customer would order two PS/2 terminators and two Sun USB terminators.

KVM Expander

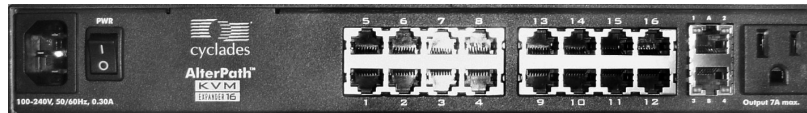
The AlterPath KVM Expander is designed to connect to the primary KVM/net to increase the number of ports that a primary KVM/net can manage.

Note: The AlterPath KVM Expander is compatible with the KVM/net Plus, the KVM/net, and the KVM. The term primary KVM unit refers to the three types of KVM units.

Front view of the AlterPath KVM Expander:



Back view of the AlterPath KVM Expander 16:



The following sections offer an introduction to the KVM Expander:

- “KVM Expander Features” on page 53
- “KVM Expander Models and Components” on page 54
- “Adding the KVM Expander to the KVM/net Unit’s List of Cascaded Devices” on page 59
- “Upgrading the KVM Expander Microcontroller Code” on page 59

KVM Expander Features

The KVM Expander has no CPU, memory, or Flash; therefore, it relies on the intelligence of the primary KVM unit to control its KVM ports, making for a simple processing core as well as a cost-effective method of cascading a KVM/net Plus, a KVM/net, or a KVM.

The KVM Expander does support the following features:

- Allows the connection of 8 or 16 servers
See “KVM Expander Models and Components” on page 54 for more details.
- Supports all existing Terminators
See “KVM Terminator Usage and Types” on page 51 for more details.
- Is compatible with the AlterPath KVM, KVM/net, and KVM/net Plus units
See “Cascaded Devices” on page 24 for more details.
- Operates with up to two input ports – User A and User B
See “Ports on the KVM Expander” on page 55 for more details.
- Supports horizontal or vertical rack mounting
See “Setting Up the KVM Expander” on page 111 for more details.
- Allows daisy-chaining of KVM Expander units through its AC power outlet
See “To Power On Devices Daisy Chained to the KVM Expander’s Power Outlet” on page 114 for more details.
- Displays port status with LEDs.
See “LEDs on the KVM Expander” on page 56

KVM Expander Models and Components

The KVM Expander comes in two models, which differ only in number of KVM ports:

Table 1-18: KVM Expander Model Numbers and Port Options

Model Number	Part Numbers	KVM Ports
8	ATP4208	8
16	ATP4216	16

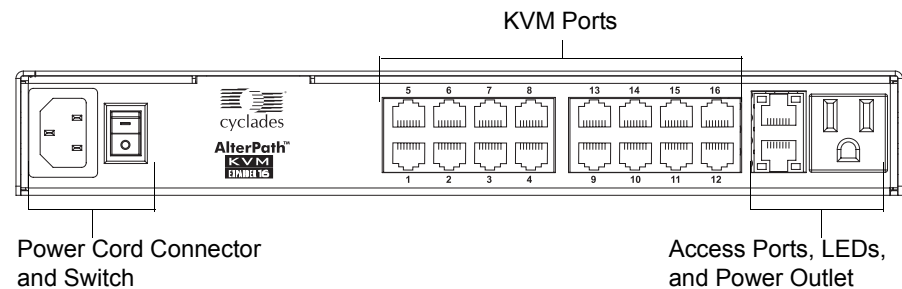


Figure 1-11: KVM Expander Back Panel Components

The following sections explain the components of the KVM Expander:

- “Ports on the KVM Expander” on page 55
- “LEDs on the KVM Expander” on page 56
- “Power Outlets on the KVM Expander” on page 56

Ports on the KVM Expander

The KVM Expander has two CAT5 access ports and either 8 or 16 KVM ports.

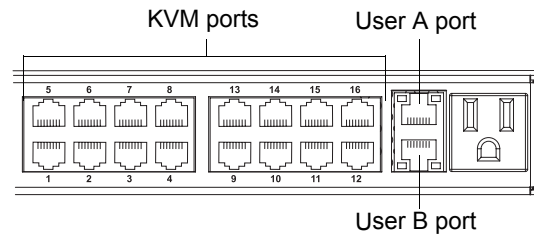


Figure 1-12:Ports on the KVM Expander Back Panel

Table 1-19:KVM Expander Port Types

Port Type	Use and Connection Information
User A and User B	The access ports can be connected with an RJ-45 cable to KVM ports on the primary KVM unit. Once the KVM Expander is configured as a cascaded device on the master KVM unit, users can connect to one or both ports. Each port allows one connection to a server plugged in to the KVM Expander, so a maximum of two server connections can be made at one time. See “Installing the AlterPath KVM Expander” on page 108.
KVM ports	KVM ports on the KVM Expander work exactly as the KVM ports on the KVM/net: They allow the connection of a CAT 5 cable to a terminator, which is connected to a USB Sun server running Solaris or a PC running a Windows, Linux, or other open source operating system. See “KVM Ports” on page 10 for more background information on KVM ports. See “Connecting Servers to the KVM Ports” on page 70 for information on connecting servers to the KVM ports.

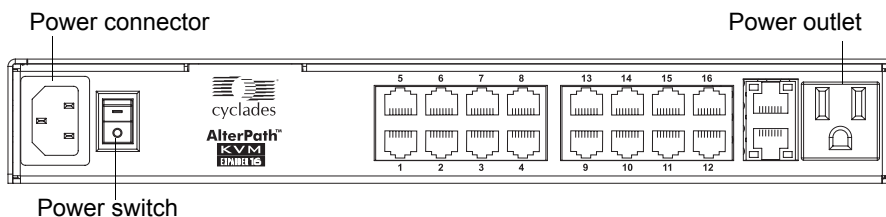
LEDs on the KVM Expander

The two LEDs on either side of the User A and User B ports on the KVM Expander blink when data activity occurs through the User A or User B port respectively.

Power Outlets on the KVM Expander

The KVM Expander has a power connector for power input and a power outlet for daisy chaining additional KVM Expanders or any other device.

Caution! The total amount of power consumed by devices daisy-chained to the KVM Expander must not exceed seven amps.



Cascading a KVM Expander

The KVM Expander can support up to two users simultaneously accessing its KVM ports. In a two-user configuration, a primary KVM switch uses two connections for each KVM Expander-to-primary KVM switch configuration:

- User A port – One CAT5 cable between a KVM port on the primary KVM unit and the User A port on the KVM Expander
- User B port – One CAT5 cable between a KVM port on the primary KVM unit and the User B port on the KVM Expander

In a single user configuration, only one CAT5 cable is connected from a KVM port on the primary KVM unit to either of the users ports on the KVM Expander.

The following diagram displays a KVM Expander cascaded from a KVM/net.

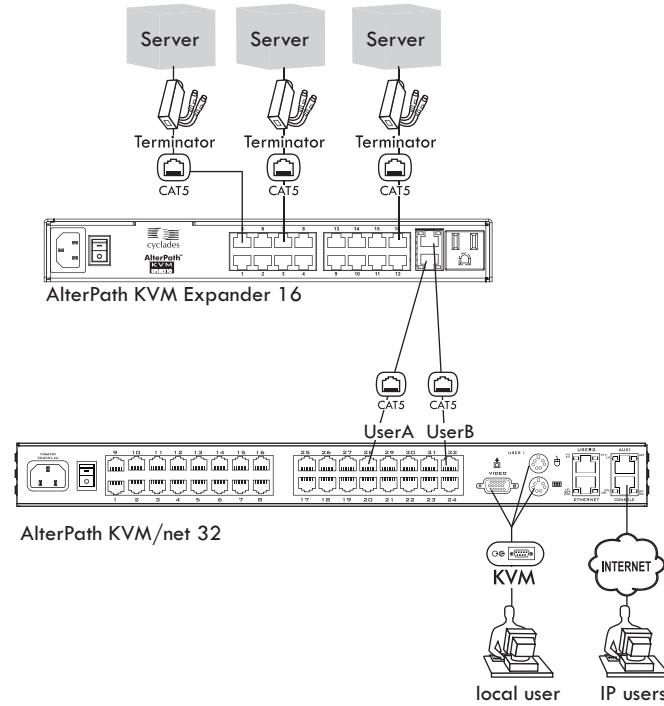


Figure 1-13:Connecting a KVM Expander to the KVM/net

Introduction

The following table shows the maximum number of servers a primary KVM/net Plus, KVM/net, or KVM can support when cascaded with a KVM Expander 8 or a KVM Expander 16.

Table 1-20:Maximum Number of Supported Servers

KVM Unit	Model Number	KVM Expander and Model Number	Maximum Number of Servers
KVM	32	KVM Expander 16	512
KVM	32	KVM Expander 8	256
KVM/net	16	KVM Expander 16	256
KVM/net	16	KVM Expander 8	128
KVM/net Plus	1601/1602/1604	KVM Expander 16	256
KVM/net Plus	1601/1602/1604	KVM Expander 8	128
KVM/net Plus	3201/3202/3204	KVM Expander 16	512
KVM/net Plus	3201/3202/3204	KVM Expander 8	256

Adding the KVM Expander to the KVM/net Unit's List of Cascaded Devices

Once the administrator connects the KVM Expander to the primary KVM unit, the administrator must add the Expander to the primary unit's list of cascaded devices. Using the KVM/net Web Manager in Expert Mode, go to: Configuration>KVM>Devices to see the form displayed in the following figure.

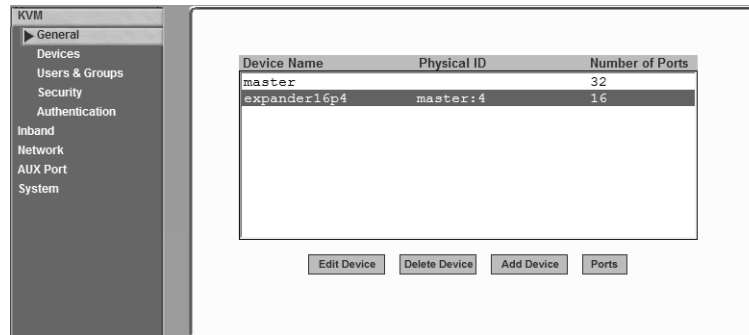


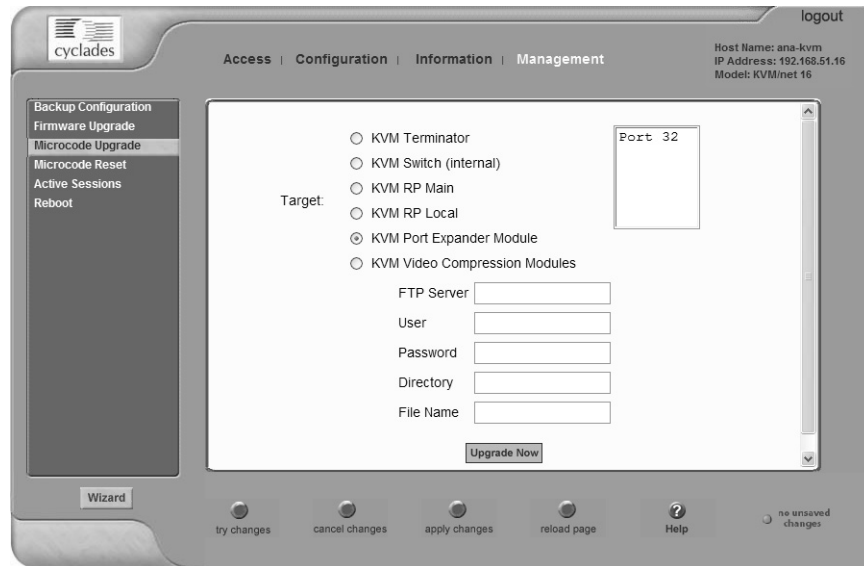
Figure 1-14:Devices Form on KVM/net Web Manager

See “Configuring Cascaded KVM Units” on page 166 for instructions on adding, deleting, and modifying cascaded devices.

Upgrading the KVM Expander Microcontroller Code

Once a KVM Expander is installed and configured, administrators can use the Microcode Update form on the primary KVM unit to upgrade the microcode for a KVM Expander. Using the KVM/net Web Manager in Expert Mode, go to: Management > Microcode Update to see the form displayed in the following figure.

Introduction



The screenshot shows the 'Microcode Upgrade' form in the KVM/net Web Manager. The interface includes a 'cyclades' logo, navigation tabs for 'Access', 'Configuration', 'Information', and 'Management', and a 'logout' link. The host information is 'Host Name: ana-kvm', 'IP Address: 192.168.51.16', and 'Model: KVM/net 16'. A sidebar on the left lists options: 'Backup Configuration', 'Firmware Upgrade', 'Microcode Upgrade' (selected), 'Microcode Reset', 'Active Sessions', and 'Reboot'. The main form area has a 'Target:' section with radio buttons for 'KVM Terminator', 'KVM Switch (Internal)', 'KVM RP Main', 'KVM RP Local', 'KVM Port Expander Module' (selected), and 'KVM Video Compression Modules'. There is a 'Port 32' label and a text input field. Below the target selection are input fields for 'FTP Server', 'User', 'Password', 'Directory', and 'File Name'. An 'Upgrade Now' button is at the bottom of the form. At the very bottom of the page are buttons for 'Wizard', 'try changes', 'cancel changes', 'apply changes', 'reload page', 'Help', and 'no unsaved changes'.

Figure 1-15:Microcode Update Form on KVM/net Web Manager

See “Microcode Upgrade” on page 260 for instructions on updating the microcode on a KVM Expander.

User Access

The primary KVM switch takes care to prevent the same Server port from being switched ON by both user ports. If this happens, the last USER to access the Server port will have **read-only** access (*i.e.*, the user will have no access to the keyboard and mouse).

AlterPath KVM RP

While using the AlterPath KVM RP, an administrator has full access to the OSD menus, so all local administration tasks can be performed in an office or at any other location up to 500 feet away from the KVM/net. In addition, you do not need a dedicated monitor, keyboard, and mouse to use the RP; the RP box allows you to use the monitor, keyboard, and mouse of your regular workstation and use keyboard shortcuts to toggle between the view at your local work station and the view of the KVM/net. The RP also offers keyboard shortcuts to manage the extended local access to the KVM/net. The following diagram displays the connections between the RP, the KVM/net, and the local keyboard, monitor, and mouse. The AlterPath KVM RP is available in one model whose part number is ATP4710.

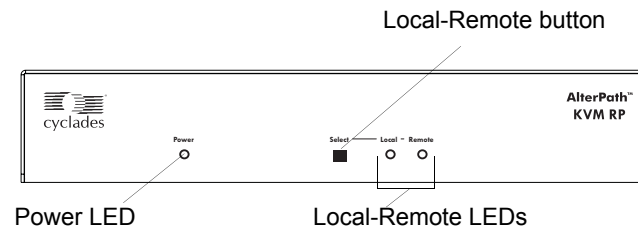


Figure 1-16:KVM RP Front

Connectors on the Back of the KVM RP

The RP has a power supply and a User, a PC, and a Remote User port as displayed in the following figure.

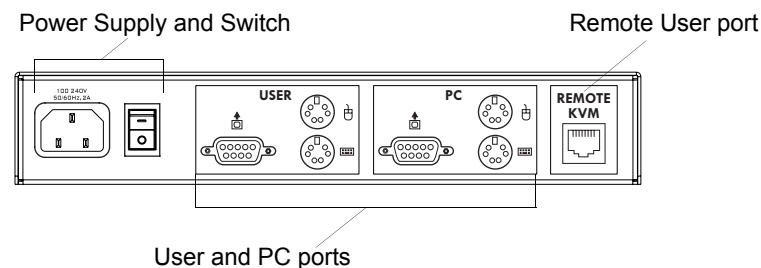


Figure 1-17:KVM RP Back Panel

Introduction

The following table offers more details about the use of and cables for each port on the back of the RP.

Table 1-21:KVM RP Port Types

Port Type	Use and Connection Information
Remote User	Its RJ-45 connection can be connected by a CAT5 cable to the User 2 port on the KVM/net.
User [PS/2 and VGA]	Keyboard, video, and mouse (KVM) management port. Includes two PS/2 ports and a VGA port, which can be connected with a KVM cable to the PS/2 ports and a VGA port on the back of the computer at the local work station.
PC [PS/2 and VGA]	Keyboard, video, and mouse (KVM) management port. Includes two PS/2 ports and a VGA port, which can be connected to a local station's mouse, keyboard, and monitor.

Chapter 2

Installing the KVM/net

This chapter outlines and described tasks for installing the KVM/net and provides other important installation-related information.

The following table lists the basic installation tasks in the order in which they should be performed and shows the page numbers where the tasks are described in more detail.

1	Review the Contents of the Shipping Box	Page 65
2	Set Up the KVM/net	Page 67
3	Make an Ethernet connection	Page 69
4	Connect computers and other devices to be managed through the KVM/net	Page 70
5	Make a direct connection (terminal or local monitor, keyboard, and mouse) to the KVM/net to prepare for basic network configuration	Page 74
6	Power on the KVM/net and connected devices	Page 75
7	Perform basic network configuration (using the wiz command or OSD network screen)	Page 76
8	Finish configuration and manage the connected devices using the Web Manager	Page 89

Installing the KVM/net

Also see the following instructions for setting up the KVM/net:

Changing Default Passwords	Page 90
Enabling Access to the Web Manager without Making a Direct Connection	Page 92
Preconfiguring the KVM/net for Remote Installation	Page 95
Additional Configuration Tasks	Page 96

Perform the optional procedures in “Installing KVM/net-related Products and Components” on page 103 if you are installing an intelligent power management device (IPDU), an external modem, an AlterPath Remote Presence (RP), an AlterPath KVM Expander, or an other cascaded KVM unit.

Shipping Box Contents AlterPath KVM/net

The shipping box for the KVM/net contains the KVM/net along with the items shown in Table 2-1. The entry for each part provides an illustration, its part number (P/N), description, and purpose. You can use check boxes to check off each item, and you can use the part numbers from this table to reorder any of the parts.

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

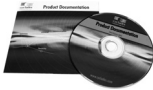
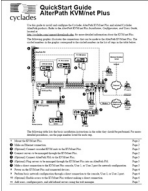



<input checked="" type="checkbox"/>	Item	P/N	Description	Purpose
<input type="checkbox"/>		PAC0226	Documentation CD	PDF copies of this guide and all other Cyclades product documents.
<input type="checkbox"/>		PAC0303	<i>AlterPath KVM/net Quick Start Guide</i>	Basic installation guide for experienced users in printed format.
<input type="checkbox"/>		CAB0010	3-pin power cord	Use to plug into a grounded AC power outlet. For other types of power sources, contact Cyclades sales for other cord options.

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

<input checked="" type="checkbox"/>	Item	P/N	Description	Purpose
<input type="checkbox"/>		CAB0018	RJ-45 to RJ-45 7ft. CAT5 cable	Use for the following: <ul style="list-style-type: none"> • To connect a server to a KVM port (with the appropriate terminator from Table 1-17 on page 51). See “Connecting Servers to the KVM Ports” on page 70. • To connect an Ethernet port to the LAN. See “To Make an Ethernet Connection” on page 69. • To connect a terminal to a console port. See “To Connect to the Console Port” on page 74. • To connect an IPDU or external modem to the AUX port. See “Connecting AlterPath PMs to the KVM/net” on page 106 and “Connecting an External Modem” on page 103.
<input type="checkbox"/>		HAR0370	2 - Mounting brackets with 8 - screws (2 spares)	Use to mount the KVM/net to a rack or wall. See “To Mount the KVM/net” on page 67.

When ordering the KVM/net , customers also order one KVM terminator for each server to be connected to one of the KVM ports. The number and types of KVM terminators in each order are based on the number of KVM ports on the KVM/net 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 51.

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

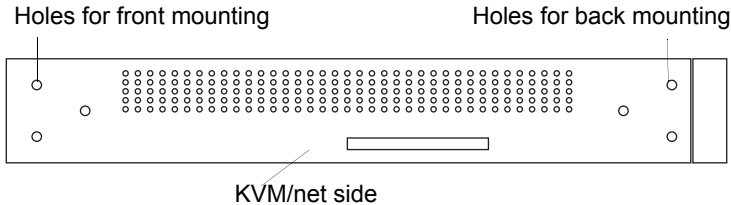
Setting Up the KVM/net

You can mount the KVM/net on a rack or place it on a desktop or other flat surface. Two brackets are supplied with six hex screws for attaching the brackets to the KVM/net for mounting.

- If you are not mounting the KVM/net, place the KVM/net on a desk or table.
- If you are mounting the KVM/net, obtain a hex screwdriver and appropriate nuts and bolts before starting the following procedure.

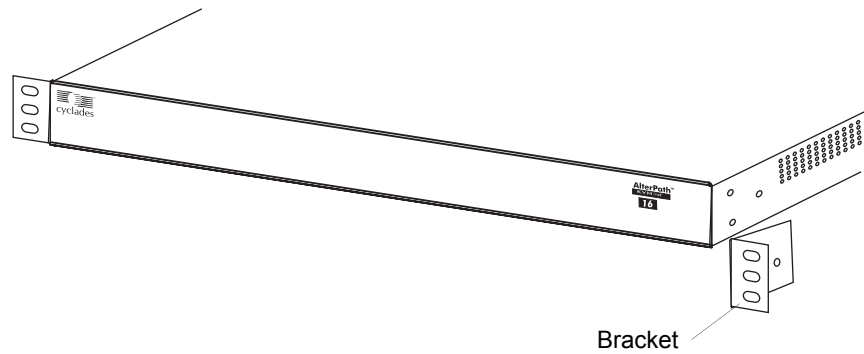
▼ To Mount the KVM/net

1. Connect the two supplied brackets to the KVM/net, connecting one bracket to each side of the box.
 - a. Decide whether you need to mount the KVM/net by the front or back and locate the appropriate sets of holes on the KVM/net.

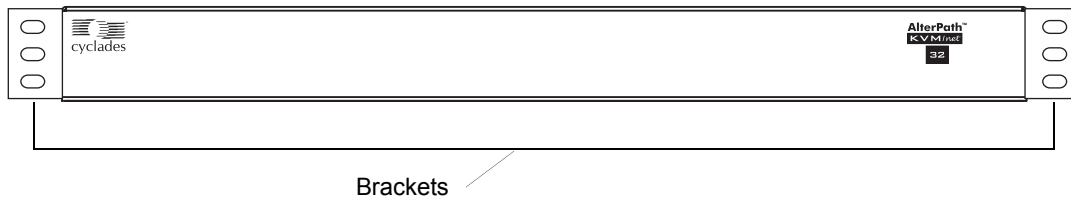


- b. For each bracket, insert a screw through each of the three holes on the bracket into the appropriate holes at either the front or back of the KVM/net.

Installing the KVM/net



The following figure shows the bracket flanges on the front of the KVM/net after the brackets are installed.



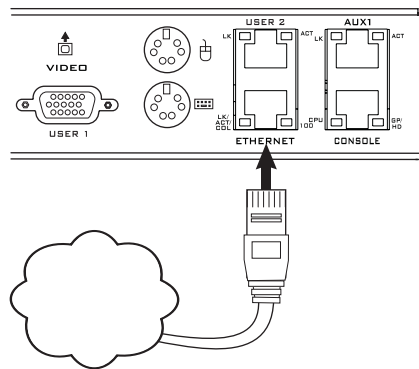
- c. Use a hex screwdriver to tighten the screws.
- 2.** Use screws or nuts and bolts as appropriate to mount the KVM/net on a rack.

Making an Ethernet Connection

Make an Ethernet connection to the KVM/net in order to have Ethernet access to the Web Manager and remote access to devices connected to the KVM/net.

▼ **To Make an Ethernet Connection**

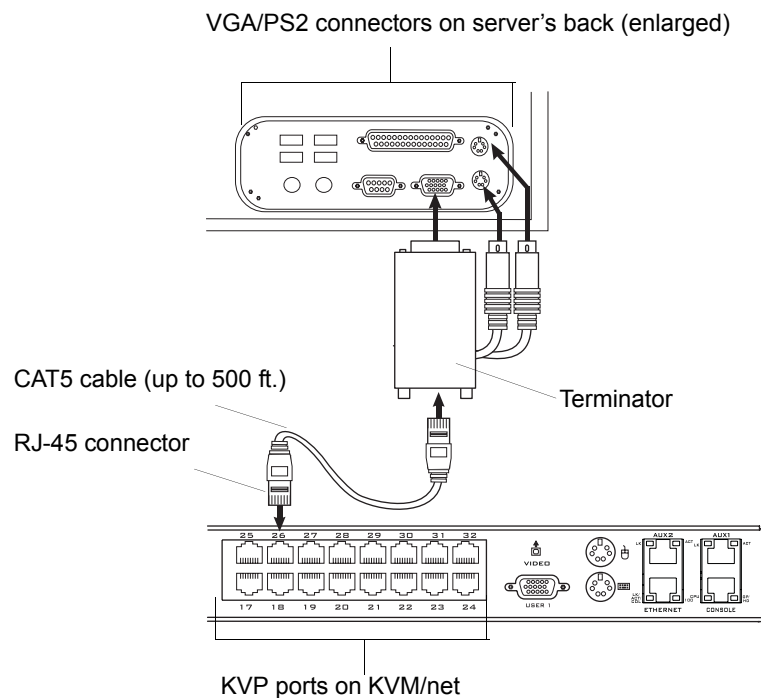
1. Connect one end of an Ethernet cable to your local area network (LAN).
2. Connect the other end to the Ethernet port on the KVM/net.



Remote connections can also be made through an external modem connected to the AUX port. See “Modem Connections” on page 312 for background information and instructions.

Connecting Servers to the KVM Ports

You need to connect a KVM terminator to every server before connecting it to a KVM port. Three terminator types are available: PS/2 PC for servers with VGA and PS/2 connectors, USB PC for servers with VGA and USB connectors, and USB Sun terminators for Sun servers with USB connectors. See “KVM Terminator Usage and Types” on page 51 for more details about the KVM Terminators, which are ordered and shipped with the KVM/net.



Note: The KVM/net components are hot-pluggable, but components of connected devices, such as the PS/2 keyboard and mouse ports on a computer, may not be hot-pluggable. Turn off power to all devices before connecting them. Power on connected devices again only after the KVM/net is powered on.

Follow the procedures below when connecting computers to KVM ports on KVM/net or on the KVM Expander. For connecting AlterPath PMs or

cascaded KVM units, see Chapter 3, “Installing KVM/net-related Products and Components.”

Note: KVM port connections rely on the CAT5 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 better and that the patch panel has all four pairs wired.

▼ ***To Prepare to Connect Devices to the KVM/net***

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

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

- All devices are installed and fully configured.
- User accounts with the appropriate permissions level exist on each device and you have the computer’s root password for users who need root access to manage the device through the KVM/net.
- On all computers to be connected to KVM server ports, the mouse settings have been modified, as described in “Avoiding Conflicting Mouse Settings” on page 96.

2. If a device is to use remote authentication, do the following steps:

- a. Make sure that the following prerequisite configuration is complete:

- Authentication servers are installed and fully configured.
- You have the root password for all users who need root access to manage the device through the KVM/net.

Note: You may want to assign different passwords for a device’s administrator on the KVM/net and on the device’s remote authentication server. If the administrator logs into the device using the password for the authentication server and log in fails, the failure can indicate that the authentication server is down and that the device’s administrator should be notified to take action.

- b. Obtain the information you need to identify the authentication server on the KVM/net from the server’s administrator.

Installing the KVM/net

- c. After the KVM/net is installed, make sure to specify the desired authentication method for the ports that are connected to each device.

See “Authentication” on page 44 for background information and see “Configuring an Authentication Method” on page 185 for the procedure.

3. Because some components of connected equipment may not be hot-pluggable, make sure all devices are powered off.

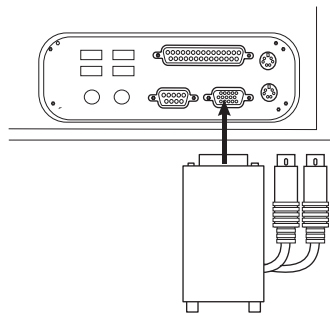
▼ **To Connect Computers to KVM Ports**

Do these steps after completing “To Prepare to Connect Devices to the KVM/net” on page 71.

1. Select the appropriate terminator.

Three terminator types are available: PS/2 for PCs, USB for PCs, and USB for Sun systems. See “KVM Terminator Usage and Types” on page 51 for more details about the terminators, which are ordered and shipped with the KVM/net.

2. Connect the terminator’s VGA (HD-15 male) connector to the computer’s VGA (monitor) port, tightening both screws firmly but not over-tightening.

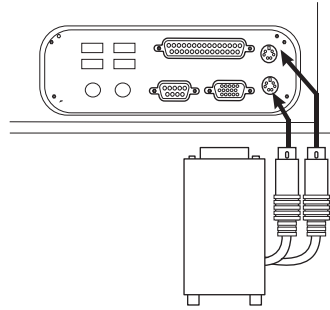


3. If the PC’s VGA port is recessed too far for easy access, insert a VGA mini extender before attempting to connect the VGA connector.

The VGA DB-9 mini extender (part number ADB0035) can be ordered separately from Cyclades.

Connecting Servers to the KVM Ports

4. To complete the connection of a PS/2 terminator to a PC, connect the terminator's purple and green connectors to the purple keyboard port and green mouse port on the PC.



5. To complete the connection of a USB terminator to a PC or Sun computer, plug the USB connector from the terminator to the computer's USB port.
6. To extend the connection from the computer to the KVM/net, connect an RJ-45 to RJ-45 CAT5 cable up to 500 feet long to the terminator.
7. Connect the RJ-45 connector on other end of the cable to a KVM port on the KVM/net.
8. Repeat Step 1. through Step 7. for all computers to be connected to the KVM ports.
9. If any user is using a PC with Windows XP server pack 2 installed and Internet Explorer 5 or 6 to remotely administer a connected device, make sure the procedure under "Avoiding Internet Explorer Conflicts" on page 100 has been done on the PC.
10. If this is a first-time installation, go to "Making a Direct Connection for Network Configuration" on page 74.

Making a Direct Connection for Network Configuration

The system administrator must specify basic network settings on the KVM/net before administrators can connect to and manage the unit and the connected devices through a browser. To prepare to perform necessary basic network configuration, make a direct connection to the KVM/net by doing one of the following:

- Connect a terminal or computer to the CONSOLE port.
See “To Connect to the Console Port” on page 74.
- Connect a keyboard, monitor, and mouse to the monitor, keyboard, mouse connectors on the KVM/net.
See “To Connect to the User 1 Management Port” on page 75.

See “Enabling Access to the Web Manager without Making a Direct Connection” on page 92, if desired, for other procedures that require advanced system administration expertise.

▼ *To Connect to the Console Port*

Perform the following steps to connect a computer to the console port of the KVM/net. This procedure assumes that you know how to use a terminal emulation program.

On 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 Solaris or Linux, make sure that a compatible terminal emulator such as Kermit or Minicom, is installed.

1. Connect an RJ-45 serial cable to the console port on the KVM/net.
2. Connect the other end to a USB serial adapter or DB-9 connection on the computer.
3. Using a terminal emulation program installed on a computer, start a session with the following console port settings:

Serial Speed: **9600** bps

Data Length: **8** bits

Parity: **None**

Stop Bits: **1**

Flow Control: **None**

ANSI emulation

4. Go to Chapter 2. “Powering On the KVM/net and Connected Devices” on page 2-75.

▼ **To Connect to the User 1 Management Port**

Connect a keyboard, monitor, and mouse to the User 1 port on the right back of the KVM/net.

1. Plug the station's monitor, keyboard, and mouse cables to the Keyboard, Video, and Mouse connectors, labelled User 1, on the KVM/net.
2. Go to “Powering On the KVM/net and Connected Devices” on page 75.

Powering On the KVM/net and Connected Devices

▼ **To Power On the KVM/net**

1. Make sure the KVM/net's power switch is off.

The power is off when the side of the power switch with the circle is pressed down.

2. Plug in the power cable.
3. Turn the KVM/net's power switch on.

The KVM/net beeps once.

▼ **To Power On Connected Devices**

Do this after “Connecting Servers to the KVM Ports” on page 70.

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

Performing Basic Network Configuration

The administrator must specify basic network settings before regular users can connect to and manage the KVM/net and the connected devices through a browser. Do one of the following to assign a fixed IP address to the KVM/net, and to specify the netmask and other networking parameters:

- Through a console connection, log in and use the wiz command.
See “Configuring Basic Networking Using the wiz Command” on page 77.
- Through a local KVM connection, log into the OSD and configure networking through the network screen.
See “Configuring Basic Networking Using the OSD” on page 80.

Before you start, collect the following network information from the administrator of the network where the KVM/net is to reside.

<input type="checkbox"/> Hostname:	
<input type="checkbox"/> KVM/net’s public IP address:	
<input type="checkbox"/> Domain name:	
<input type="checkbox"/> DNS server’s IP address:	
<input type="checkbox"/> Gateway IP address:	
<input type="checkbox"/> Network mask:	
<input type="checkbox"/> KVM/net’s MAC address (from the label on the bottom):	
<input type="checkbox"/> NTP server’s IP address (if you are using a time/date server):	

Note: The following procedures tell you to disable DHCP. Enabling DHCP requires a DHCP server at your site. When DHCP is enabled, anyone administering the KVM/net or its connected devices needs access to the DHCP server to look up the current IP address every time before using the Web Manager. See “Considerations When Choosing Whether to Enable DHCP” on page 50 for

more details and see “To Use a Dynamic IP Address to Access the Web Manager” on page 93 for the tasks that must be performed.

Configuring Basic Networking Using the *wiz* Command

The following procedures require a hardware connection already made between the KVM/net’s console port and the COM or USB port of a computer, as described under “To Connect to the Console Port” on page 74.

▼ To Log Into the KVM/net Through the Console

From your terminal emulation application, log into the console port as root.

```
KVM/net login: root
Password: cyclades
```

As shown in the previous screen, the default password is “cyclades.” If the password has been changed from the default, use the new password.

▼ To Change the Password Through the Console

If the default password “cyclades” is still in effect, change the root password.

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

1. Enter the **passwd** command.

```
[root@KVM/net /]# passwd
```

2. Enter a new password when prompted.

```
New password: new_password
Re-enter new password: new_password
Password changed
```

▼ **To Use the `wiz` Command to Configure Network Parameters**

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

```
[root@KVM/net /]# wiz
```

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

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

3. Press Enter to accept default hostname, otherwise enter your own hostname.

```
Hostname [KVM/net]: boston_branch_kvm
```

4. Press 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 KVM/net.

```
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. To apply and confirm these parameters, see “To Apply and Confirm the Network Parameters Defined Using the wiz Command” on page 79.

▼ **To Apply and Confirm the Network Parameters Defined Using the wiz Command**

This procedure must be completed immediately after defining network parameters using the wiz command as described in “To Use the wiz Command to Configure Network Parameters” on page 78

1. 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 : kvm
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] :
```

2. Enter **y** if the values shown are correct, or press Enter and go back to Step 4. Unresolved to make any desired changes.

3. The following prompt appears when “y” is entered.

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

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

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

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

6. The new network parameters display.

7. Log out from the terminal session.

Installing the KVM/net

8. In a HyperTerminal application on a Windows PC, go to “File > Exit”.
9. If performing a first-time installation, go to Chapter 2. “Completing Configuration Using the Web Manager” on page 2-89.

Configuring Basic Networking Using the OSD

This procedure requires a hardware connection already made between the KVM/net’s KVM management port and a local monitor, keyboard, and mouse, as described under “To Connect to the User 1 Management Port” on page 75. After the KVM/net and monitor are powered on, the AlterPath Viewer appears displaying the OSD login screen.

Production Note: get new screen shot



The following table shows how to perform common actions described in the following procedures when working with the OSD.

Table 2-2: OSD Equivalents for Common Actions

Action.	OSD Equivalent.
Press OK.	Tab to the OK button and press the Enter key on your keyboard.
Enter <any value>.	Type the value in the appropriate field and press the Enter key.
Save changes.	Tab to the Save button and press the Enter key.
Select <an option>.	Press an arrow key to navigate. Select the menu option and then press the Enter key.

Table 2-2: OSD Equivalents for Common Actions (Continued)

Action.	OSD Equivalent.
Go to a specific screen, as in: “Go to ‘Configure > Users and Groups > Local Users > Change Password’.”	From the Main menu, select the first option shown in the menu path; “Configure” in the example. On the next menu, select the next option shown after the > (right angle bracket); “Users and Groups” in the example. Repeat until you select the last option in the menu path.
Exit the OSD.	Click the X box on the upper right of the viewer. If you are on the Main Menu, you can select Exit.

Note: If your keyboard has a Return key instead of an Enter key, press the “Return” key when you see “Enter.”

▼ To Log Into the OSD

1. On the OSD login screen, enter “admin” as the Login name.
2. Enter the password.

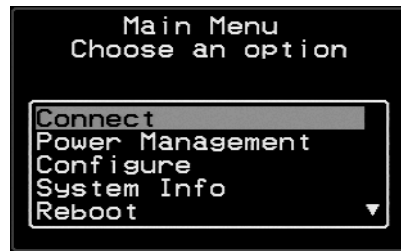
The default password is “cyclades.” If the password has been changed from the default, use the current password.



3. Press Enter.

The OSD Main Menu appears.

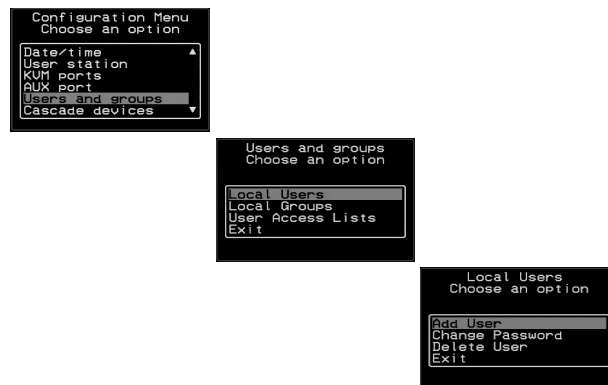
Installing the KVM/net



4. If you are performing an initial configuration of basic networking parameters, go to “To Change a Password Using the OSD” on page 82; otherwise, go to “To Configure Network Parameters Using the OSD” on page 84.

▼ To Change a Password Using the OSD

1. From the OSD Main Menu, go to Configure > Users and Groups > Local Users > Change Password.



Warning! If the “root” and “admin” passwords have not been changed, change them now. Changing the default password closes a security hole that could be easily exploited.

2. Select the user name from the list of users on the User Database screen.



3. Enter a new password.

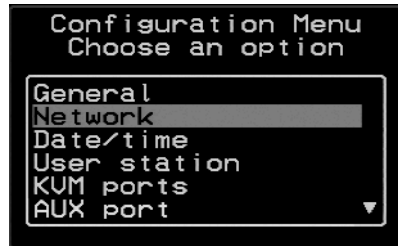


4. Re-enter the new password.
The password confirmation dialog box appears.
5. Press Enter.
The Local Users menu appears.
6. Select Exit or press the Esc key to exit the Local Users menu.
You can use the Exit or Cancel option or the Esc key to exit any window on the OSD.
7. If you are performing an initial configuration of basic networking parameters, go to: To Configure Network Parameters Using the OSD.”
8. Otherwise, go to the appropriate menu option for your next task.

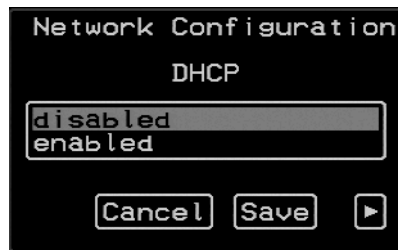
Installing the KVM/net

▼ **To Configure Network Parameters Using the OSD**

1. From the OSD Main Menu, go to Configure > Network.

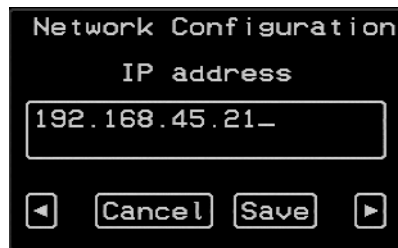


The DHCP form appears.



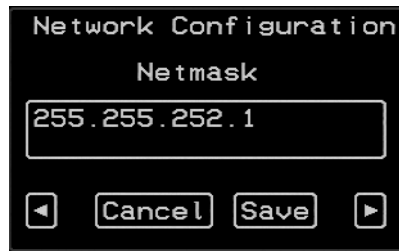
2. Select the “disabled” option and press Enter.

The IP address form appears.

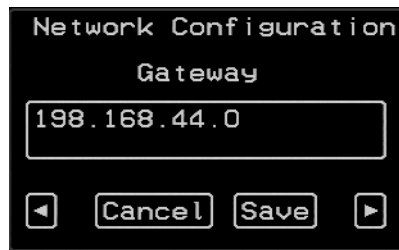


3. Enter the IP address for the KVM/net and press Enter.

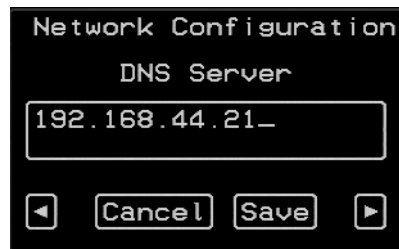
The Netmask form appears.



4. Enter the netmask (in the form 255.255.255.0) and press Enter.
The Gateway form appears.

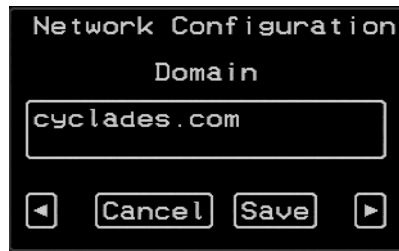


5. Enter the IP address for the gateway and press Enter.
The DNS Server form appears.



6. Enter the IP address for the DNS server and press Enter.
The Domain form appears.

Installing the KVM/net



7. Enter the domain name and press Enter.

The Hostname form appears.



8. Enter the hostname for the KVM/net and save the changes to complete the basic network configuration.

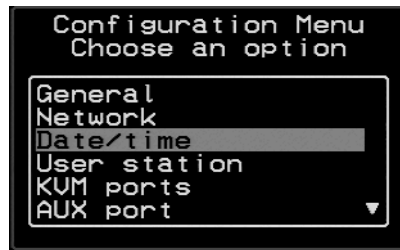
The Configuration menu appears.

- To configure an NTP (network time protocol) server or to enter the date and time manually, go to “To Set the Time and Date Using the OSD” on page 87.
- If you do not wish to configure the time and date at this time, and if you are performing an initial configuration of basic networking parameters, go to: “Completing Configuration Using the Web Manager” on page 89.
- Otherwise, go to the appropriate menu option for your next task or exit from the OSD.

▼ **To Set the Time and Date Using the OSD**

1. From the Main menu of the OSD, go to Configure.

The Configuration menu appears.



2. Select Date/time.

The Date/time conf. form appears.



3. To enable the NTP time and date server, do the following.

- a. On the Date/time conf. form, select the “enabled” option.

The NTP server screen appears



- b. Enter the IP address of the NTP server.
- c. Save the changes.

Installing the KVM/net

4. To enter the date and time manually, do the following.

- a. On the Date/time conf. form, select disabled.

The Date entry screen appears.



The screenshot shows a terminal window titled "Date/time Conf.". Below the title, it says "Date YYYY/MM/DD". A text input field contains the date "2005/01/25". At the bottom of the window, there are four buttons: a left arrow, "Cancel", "Save", and a right arrow.

- b. Enter the date in the format shown and press Enter.

The Time entry screen appears.



The screenshot shows a terminal window titled "Date/time Conf.". Below the title, it says "Time hh:mm:ss". A text input field contains the time "11:39:09_". At the bottom of the window, there are four buttons: a left arrow, "Cancel", "Save", and a right arrow.

- c. Enter the time in the format shown and save the changes.

If you are performing an initial configuration of basic networking parameters, go to: "Completing Configuration Using the Web Manager" on page 89.

Otherwise, go to the appropriate menu option for your next task.

Completing Configuration Using the Web Manager

The “admin” user can administer the KVM/net and its connected devices through the Web Manager without doing any additional configuration.

The following list shows other common configuration tasks:

- Enable direct login to ports from the Web Manager login screen
- Set up local or remote data buffering (to save console input to a log file) and specify alarms
- Set up logging of system messages to a syslog server
- Configure power management for the AUX port if the port is connected to an optional AlterPath PM or other supported IPDU device
- Choose among authentication methods and specify authentication servers
- Specify optional encryption levels
- Configure rules for a firewall
- Configure a time and date (NTP) server or set the time and date manually

See “Web Manager for Administrators” on page 123 for procedures for performing the common KVM/net administration tasks listed in this section.

Following is a brief list of ways the admin can assign tasks to other users:

- Let other users manage servers or PMs without being able to make changes to the KVM/net configuration
- Assign users or groups to specific ports, restricting users to a limited set of devices
- Let other users share all administration of the KVM/net

Changing Default Passwords

For security purposes, the root and admin users must change their default passwords as soon as possible. Not changing the default passwords leaves a big security hole that can be exploited.

▼ **Changing admin's Default Password [Web Manager]**

1. Bring up the Web Manager.
2. Log in as admin using the default password, “cyclades”.
3. In Wizard Mode, go to **Step3: Access**.
4. Select “admin” from the Users List.
5. Click the “Change Password” button.
6. Enter the password into the New Password field.
7. Enter the password again into the Repeat New Password field.
8. Click OK when done.

▼ **Changing the Root Password [Command Line]**

1. Verify that a terminal or a computer with a terminal emulator is connected to the console port on the KVM/net.
2. From the terminal or terminal emulator, log into the console port as **root**, using the existing password. [The default password is cyclades.]

KVM login: root

Password: cyclades

- a. Enter the **passwd** command.

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

- b. Enter a new password when prompted.

```
New password: new_password
```

```
Re-enter new password: new_password  
Password changed
```

3. Save the new password by entering the **saveconf** command.

```
[root@KVM /]# saveconf
```

4. Log out.

```
[root@KVM /]# logout
```

5. Close the terminal session.
6. In a HyperTerminal application on a Windows PC, choose File > Exit or F4.

▼ **Changing Default Passwords [OSD]**

This procedure requires a hardware connection already made between the KVM/net's KVM management port and a local monitor, keyboard, and mouse, as described in "To Connect to the User 1 Management Port" on page 75. Do the following to change the passwords for the root and admin users.

1. Log into the OSD.
2. From the Main Menu, select the Configure option.
3. From the Configure Menu, select the Users and Groups option.
4. From the list of users on the User Database screen, select the user name.
5. On the "Enter the Password" screen, enter the new password.
6. On the password confirmation window, re-enter the password.
7. Select OK.

Enabling Access to the Web Manager without Making a Direct Connection

This section describes additional alternatives for enabling access to the Web Manager that do not require making a direct connection. Both of the two following approaches require an experienced administrator to configure:

- The KVM/net ships with a default IP address: 192.168.160.10. You can use the default address to bring up the Web Manager, assign a fixed IP address to the KVM/net and specify other network parameters without making a direct connection. To do so, you must temporarily change the IP address of a computer on the same subnet. See “To Use the Default IP Address to Access the Web Manager” on page 92.”
- DHCP is enabled on the KVM/net by default. If you have network access to the DHCP server for the KVM/net, and if you are able to discover the KVM/net’s dynamically-assigned IP address, you do not need to make a direct connection. Discovering the current IP address requires entering the KVM/net’s MAC address. Make a note of the MAC address, which is on a label at the bottom of the unit in the form *NN-NN-NN-NN-NN-NN*, and go to “To Use a Dynamic IP Address to Access the Web Manager” on page 93.”

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

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

1. Set up the AlterPath KVM/net Plus.
See “To Mount the KVM/net” on page 67.
2. Connect computers and other devices to be managed through the KVM/net Plus.
See “Connecting Servers to the KVM Ports” on page 70.
3. Power on the KVM/net Plus and connected devices.
See “Powering On the KVM/net and Connected Devices” on page 75.

Enabling Access to the Web Manager without Making a Direct Connection

4. On a computer that resides on the same subnet with the KVM/net Plus, change the network portion of the IP address of that computer to 192.168.160.NN, where NN is not 10, and change the Netmask to 255.255.255.0.

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

5. Bring up a browser on the computer whose address you changed, enter the KVM/net Plus' default IP address (`http://192.168.160.10`) to bring up the Web Manager, and log in.
6. To allow subsequent use of the Web Manager from any computer, go to the Wizard: "Step 1: Network Settings" to change the default IP address to a fixed public IP address and to configure the other basic network parameters and save them to Flash.
7. Restore the computer's IP address to its previous IP address.
8. Finish configuring KVM/net Plus users and ports using the Web Manager.

▼ **To Use a Dynamic IP Address to Access the Web Manager**

This procedure assumes that DHCP is enabled on the KVM/net Plus.

1. Set up the AlterPath KVM/net Plus.
See "To Mount the KVM/net" on page 67.
2. Connect computers and other devices to be managed through the KVM/net Plus.
See "Connecting Servers to the KVM Ports" on page 70.
3. Power on the KVM/net Plus and connected devices.
See "Powering On the KVM/net and Connected Devices" on page 75.
4. To obtain the KVM/net Plus' current IP address from the console port do the following:
 - a. Using the console port, log in as "root."
See "To Connect to the Console Port" on page 74 for instructions if needed.

Installing the KVM/net

- b. Execute the command

```
ifconfig eth0
```

Output similar to the following will appear. The line in bold type face labelled “inet address” lists the IP address of the KVM/net Plus:

```
eth0  Link encap:Ethernet  HWaddr
      00:60:2E:01:4F:FC
      inet addr:192.168.50.72
      Bcast:192.168.51.255
      Mask:255.255.252.0
      UP BROADCAST RUNNING MULTICAST
      MTU:1500  Metric:1
      RX packets:7282803 errors:43
        dropped:0 overruns:0 frame:43
      TX packets:167335 errors:3
        dropped:0 overruns:0 carrier:3
      collisions:0 txqueuelen:100
      RX bytes:539070845 (514.0 MiB)  TX
        bytes:18911603 (18.0 MiB)
      Base address:0xe00
```

5. To obtain the KVM/net Plus’ current IP address from the DHCP server, supply the MAC address from the bottom side of the KVM/net Plus’ chassis. (The address has the form: *NN-NN-NN-NN-NN-NN*, as in this example: 00-60-3D-01-36-B4.)
6. Finish configuring KVM/net Plus users and ports using the Web Manager.

Preconfiguring the KVM/net for Remote Installation

This section provides procedures that list the tasks for preconfiguring the KVM/net and setting it up in a separate location. You might preconfigure a KVM/net, for example, if you need to ship the KVM/net to a remote location that does not have a system administrator.

If you would prefer to have Cyclades preconfigure the KVM/net with basic network parameters at Cyclades Corporation before it is shipped, ask your Cyclades contact to put you in touch with Cyclades professional services. For a fee, they can preconfigure the KVM/net with parameters you supply.

▼ *To Preconfigure the KVM/net*

1. Perform the tasks listed in the following table to preconfigure the KVM/net for installation at another location.

Task	Where Documented
Make a direct connection to prepare for basic network configuration.	“Making a Direct Connection for Network Configuration” on page 74
Power on the KVM/net and connected devices.	“Powering On the KVM/net and Connected Devices” on page 75
Perform basic network configuration.	“Performing Basic Network Configuration” on page 76

2. If you ship the KVM/net to a remote location for installation, also send the following:
 - A record of the KVM/net’s fixed IP address and other network parameters.
 - A copy of the instructions under To Set Up a Preconfigured KVM/net.”

▼ *To Set Up a Preconfigured KVM/net*

Perform the tasks shown in the following table with a KVM/net that has been preconfigured as described in “To Preconfigure the KVM/net” on page 95. After the tasks are completed in the order shown, a remote administrator can

Installing the KVM/net

bring up the Web Manager by entering the KVM/net's fixed IP address in a browser.

Task	Where Documented
1 Set up the AlterPath KVM/net.	“Setting Up the KVM/net” on page 67
2 Make an Ethernet connection.	“Making an Ethernet Connection” on page 69
3 Connect computers and other devices.	“Connecting Servers to the KVM Ports” on page 70
4 Power on the KVM/net and connected devices.	“Powering On the KVM/net and Connected Devices” on page 75

Additional Configuration Tasks

See the following sections for other procedures.

Task	Where Documented/Notes
Avoiding Conflicting Mouse Settings	“Avoiding Conflicting Mouse Settings” on page 96
Avoiding Internet Explorer Conflicts	“Avoiding Internet Explorer Conflicts” on page 100
Assigning Your Own TCP Viewer Port Address	“Types of Ports” on page 7

Avoiding Conflicting Mouse Settings

The administrator of each computer connected to one of the KVM/net's KVM server ports must perform one of the procedures in this section. Performing the procedure prevents conflicts between the mouse settings on the connected computers and the mouse settings on computers used to do administration through the KVM/net.

Work with the administrators of computers to be connected to the KVM/net to ensure that one of the following procedures is performed, depending on the type of computer:

- “To Prevent Mouse Conflicts [Windows XP/Windows 2003]” on page 97
- “To Prevent Mouse Conflicts [Windows 2000 / ME]” on page 98
- “To Prevent Mouse Conflicts [Windows 95/98/NT]” on page 98
- “To Prevent Mouse Conflicts [Linux]” on page 99

▼ **To Prevent Mouse Conflicts [Windows XP/Windows 2003]**

1. As administrator, on the Start Menu, go to: Control Panel > Mouse > Pointer Options.
2. To disable “Enhance pointer precision,” click the check box to clear it.
3. To set the motion speed to medium, move the slider to the middle of the “Select a pointer speed” scale.
4. Go to: Control Panel > Display > Appearance > Effects
5. To disable transition effects, click both transition effects check boxes to clear them.
6. Click OK.

▼ **To Prevent Mouse Conflicts [Windows 2000 / 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, clear the **Pointer acceleration** check box.
 - c. On Windows 2000, clear 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. Clear **Use transition effects for menus and tooltips**.
 - c. Click **OK**.

▼ **To Prevent Mouse Conflicts [Windows 95/98/ NT]**

1. As administrator, on the Start menu, go to: Settings > 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 clearing “Animate windows, menus, and lists.”

▼ **To Prevent Mouse Conflicts [Linux]**

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

- Access on the KVM/net to the port where the computer is connected
 - Access as root on the connected computer
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.

Note: Repeat this procedure to synch mouse settings after every reboot of the connected computer.

Avoiding Internet Explorer Conflicts

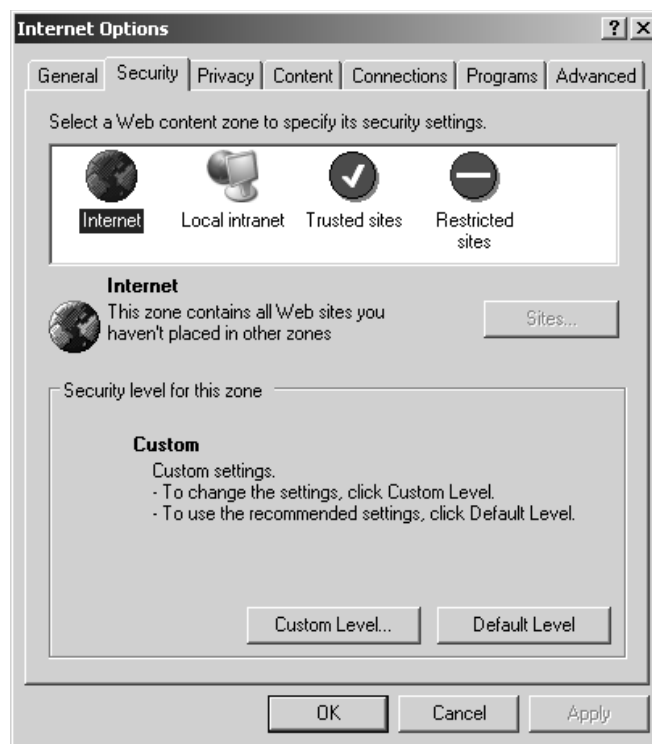
The procedure described in this section must be performed on a PC if all the following are true:

- A PC running Windows XP with Service Pack 2 is being used to remotely administer a computer connected to a KVM server port
- Internet Explorer (IE) is used to bring up the Cyclades Web Manager and the AlterPath Viewer

▼ To Modify IE Security Settings

1. From the Internet Explorer menu bar, select **Tools > Internet Options > Security Tab**.

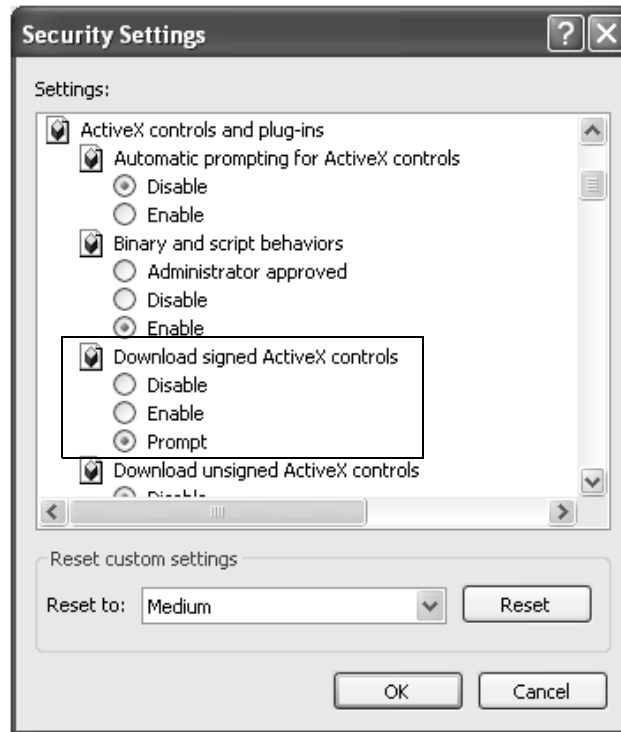
The **Security** form appears.



2. Click the **Custom Level** button.

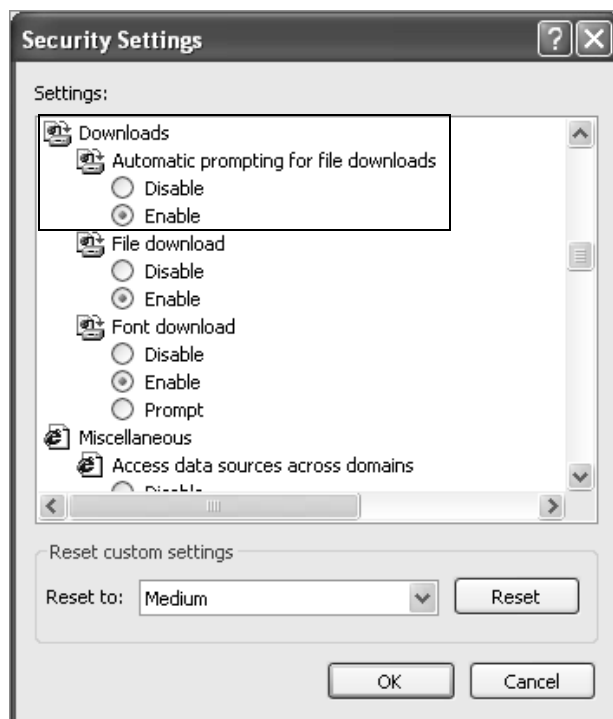
The Security Settings form appears.

3. On the Security Settings form, go to **ActiveX controls and plug-ins** > **Download signed ActiveX controls**.



4. Select either **Enable** or **Prompt**.
5. If you selected **Enable**, press the **OK** button.
6. If you selected **Prompt**, go to **Downloads** > **Automatic prompting for file downloads**, and select **Enable**.

Installing the KVM/net



7. Select the **OK** button.

Chapter 3

Installing KVM/net-related Products and Components

This chapter outlines and described tasks for installing the KVM/net-related components which are used to extend the access to and control of the KVM/net.

The following table lists the components that can be installed with the KVM/net and shows the page numbers where the tasks are described in more detail.

External modems	Page 103
AlterPath PM	Page 106
Cascaded KVM units	Page 115
AlterPath KVM Expander	Page 118
AlterPath Remote Presence	Page 118

Connecting an External Modem

You can connect a modem to the AUX port on the KVM/net. After the modem is connected and properly configured, you can use it to dial in to the KVM/net when the production network or management network is down, or when Ethernet access is unavailable.

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

This procedure requires the following cables and connectors:

- A straight through cable with an RJ-45 connector on one end and the appropriate connector or adapter (USB, DB-9, or DB-25) on the other end

Connecting an External Modem

for connecting the AUX port to the appropriate port on the external modem.

- A phone cord with RJ-11 connectors on both ends for connecting the modem to the phone line.
- 1.** Connect the RJ-45 end of the cable to the AUX port on the KVM/net.
- 2.** Connect the other end of the cable to the modem.
- 3.** Use a phone cable to connect the jack on the modem to a live telephone jack at your site.
- 4.** Configure the AUX port for PPP.

See “AUX Port” on page 239 and “To Configure the AUX Port for Use With a PM or an External Modem” on page 240.

Connecting AlterPath PMs to the KVM/net

You can control an AlterPath Power Management (PM), intelligent power distribution unit (IPDU), by connecting it to the AUX port on the KVM/net. By daisy-chaining any combination of PM models, you can control up to 128 outlets from one KVM/net.

▼ **To Connect a PM to the AUX Port**

1. Use an RJ-45 CAT5 cable to connect the AUX port on the KVM/net to the In port of your AlterPath PM.
2. Configure the AUX port for power management. See “To Configure the AUX Port for Use With a PM or an External Modem” on page 240.

Once the PM is connected, you may want to perform one or more of the following tasks:

Task	Where Documented
Install multiple PM units.	“To Connect Multiple PMs to the KVM/net” on page 107
Manage the power of devices connect to configured PM units.	<ul style="list-style-type: none">• Web Manager – “Power Management” on page 144• OSD – “Power Management Menu” on page 322
Control the power of a device while connected to it through a KVM port.	<ul style="list-style-type: none">• Web Manager – “To Power On, Power Off, or Reboot the Connected Server” on page 301• OSD – “To Power On, Power Off, Lock, Unlock, or Cycle Devices Plugged into PM Outlets” on page 310

▼ **To Connect Multiple PMs to the** KVM/net

This procedure assumes that you have one AlterPath PM connected to the AUX port of the KVM/net. See “To Connect a PM to the AUX Port” on page 106 for the procedure.

1. Use an RJ-45 CAT5 cable to connect the Out port of a PM that is already connected to the AUX port of a KVM/net to the In port of the next AlterPath PM.
2. Repeat Step 1 until you have connected the desired number of PMs.

You can control up to 128 power outlets in any combination of PM models.

See “Power Management” on page 144 for information on managing your PMs with the Web Manager.

Installing the AlterPath KVM Expander

The following table gives a high-level list of steps involved in setting up, installing, and configuring the KVM Expander with links to detailed information about each step.

1	Review the contents of the shipping box	Page 109
2	Set up the KVM Expander	Page 111
3	Connect computers to the KVM ports on the KVM Expander	Page 70
4	Connect the KVM Expander to the KVM/net	Page 117
5	Power on the KVM Expander and connected devices	Page 114
6	Add the KVM Expander to the primary KVM unit's list of cascaded devices	Page 167

Shipping Box Contents KVM Expander

The shipping box for the AlterPath KVM Expander contains the KVM Expander along with the items shown in Table 3-1. The entry for each part provides an illustration, its part number (P/N), description, and purpose. You can use check boxes to check off each item, and you can use the part numbers from this table to reorder any of the parts.

Table 3-1: KVM Expander Shipping Box Contents, Part Numbers, and Description (Sheet 1 of 2)


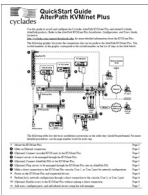



<input checked="" type="checkbox"/>	Item	P/N	Description	Purpose
<input type="checkbox"/>		PAC0226	Documentation CD	PDF copies of this guide and all other Cyclades product documents.
<input type="checkbox"/>		PAC0303	<i>AlterPath KVM/net Quick Start Guide</i>	Basic installation guide for experienced users in printed format.
<input type="checkbox"/>		CAB0010	3-pin power cord	Use to plug into a grounded AC power outlet. For other types of power sources, contact Cyclades sales for other cord options.

Table 3-1: KVM Expander Shipping Box Contents, Part Numbers, and Description
(Sheet 2 of 2)

<input checked="" type="checkbox"/>	Item	P/N	Description	Purpose
<input type="checkbox"/>		CAB0018	RJ-45 to RJ-45 7ft. CAT5 cable	Use for the following: <ul style="list-style-type: none"> To connect a server to a KVM port (with the appropriate terminator from Table 1-17 on page 51). See “Connecting Servers to the KVM Ports” on page 70. To connect the KVM Expander User A or User B ports to a KVM port on the KVM/net . See “To Connect a KVM Expander to the Primary KVM/net” on page 117 .
<input type="checkbox"/>		HAR0453	2 - Mounting brackets with 8 - screws (2 spares)	Use to mount the KVM/net to a rack or wall. See “To Mount the KVM Expander” on page 111.

When ordering the KVM Expander, customers also order one KVM terminator for each server to be connected to one of the KVM ports. The number and types of KVM terminators in each order are based on the number of KVM ports on the KVM Expander 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 51.

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

Setting Up the KVM Expander

The KVM Expander is a 1U device that can be mounted on the side of a rack or placed on a desktop or other flat surface. Two brackets are supplied with six hex screws for attaching the brackets to the KVM Expander for mounting.

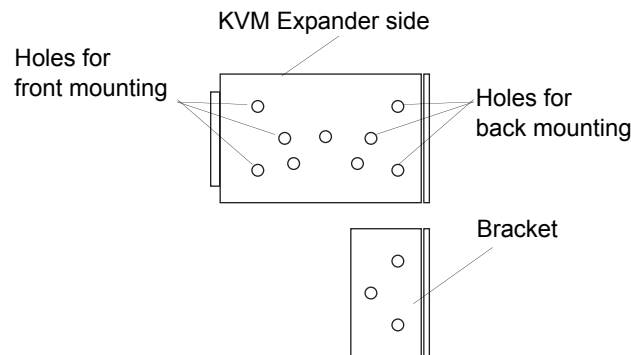
- If you are not mounting the KVM Expander, place the KVM Expander on a desk or table.
- If you are mounting the KVM Expander, obtain a hex screwdriver and the appropriate nuts and bolts before starting the following procedure.

Note: Place the KVM Expander in a location that is within the 500 feet distance allowable between the KVM/net and its connected computers. Using cables longer than 500 feet in total length can compromise performance.

▼ To Mount the KVM Expander

1. Connect the two supplied brackets to the KVM Expander, connecting one bracket to each side of the box.
 - a. Decide whether you need to mount the KVM Expander by the front or back and locate the appropriate sets of holes on the KVM Expander.

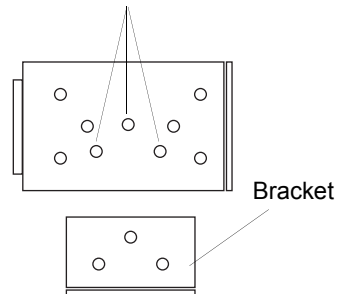
The following figure shows the angle of a bracket being installed for rack mounting.



The following figure shows the angle of a bracket being installed for wall mounting.

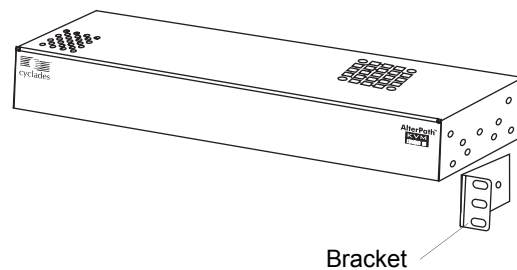
Installing KVM/net-related Products and Components

Holes for wall mounting

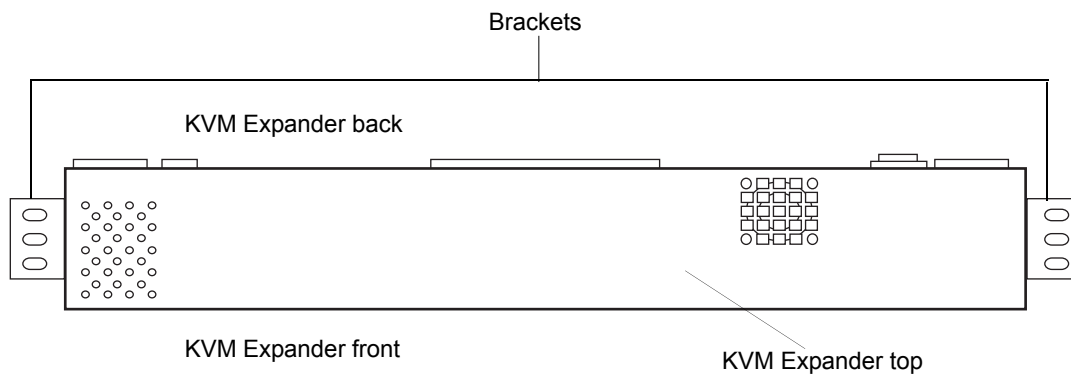


- b. For each bracket, insert a screw through each of the three holes on the bracket into the appropriate holes at either the front or back of the KVM Expander.

The following figure shows the brackets as they appear from the side and front of the KVM Expander after the brackets are installed for rack mounting.

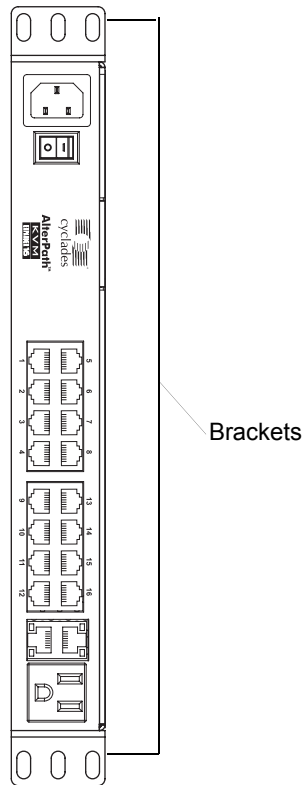


The following figure shows the brackets as they appear from the top of the KVM Expander after the brackets are installed for wall mounting.



Installing the AlterPath KVM Expander

The following figure shows the bracket flanges on the front of the KVM Expander after the brackets are installed for rack mounting.

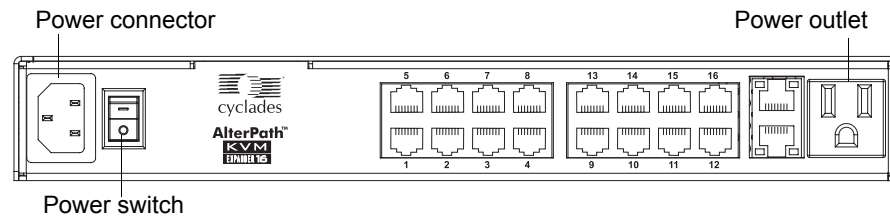


- c. Use a Phillips screwdriver to tighten the screws.
- 2.** Use screws or nuts and bolts as appropriate to mount the KVM Expander on the wall, on a rack, or in a cabinet.
- 3.** Use screws or nuts and bolts as appropriate to mount the KVM Expander on a rack.

Powering On the KVM Expander and Connected Devices

The KVM Expander has a power connector for power input and a power outlet for daisy chaining additional KVM Expanders or any other device.

Caution! The total amount of power consumed by devices daisy-chained to the KVM Expander must not exceed seven amps.



▼ To Power On the KVM Expander

1. Make sure the KVM Expander's power switch is off.

The power is off when the side of the power switch with the circle is pressed down.

2. Plug in the power cable.
3. Turn the KVM Expander's power switch on.

▼ To Power On Devices Daisy Chained to the KVM Expander's Power Outlet

1. Make sure the KVM Expander's power switch is off.

The power is off when the side of the power switch with the circle is pressed down.

2. Plug the power cable of a device in the power outlet located on the back right of the KVM Expander.
3. Turn the KVM Expander's power switch on.

▼ To Power On KVM-connected Devices

Do this after "Connecting Servers to the KVM Ports" on page 70.

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

Connecting Cascaded KVM Units to the Primary KVM/net

KVM/net supports the cascading of three types of secondary KVM devices: the AlterPath KVM, the KVM Expander, and the KVM/net. See the following sections for the appropriate instructions:

- “To Connect a Secondary KVM, KVM/net, or KVM/net Plus to the Primary KVM/net” on page 116
- “To Connect a KVM Expander to the Primary KVM/net” on page 117

Each of these cascaded devices has its own set up and installation instructions which must be performed in addition to connecting the device to the master KVM/net:

- AlterPath KVM – See the *AlterPath KVM Manual* for installation instructions.
- KVM Expander – See the “Installing the AlterPath KVM Expander” on page 108 for installation instructions.
- KVM/net – See the “Installing the KVM/net” on page 63 for installation instructions.

For background information on cascading, see “Cascaded Devices” on page 24.

▼ **To Connect a Secondary KVM, KVM/net, or KVM/net Plus to the Primary KVM/net**

1. Power off all KVM hardware and connected devices.
2. To connect to the User 2 port of a secondary KVM, KVM/net, or KVM/net Plus, do the following:
 - a. Connect one end of a CAT5 cable to a KVM port on the primary KVM/net.
 - b. Connect the other end of the CAT5 cable to the User 2 port on the secondary KVM, KVM/net, or KVM/net Plus.
3. To connect to the User 1 port of a secondary KVM, KVM/net, or KVM/net Plus, do the following:
 - a. Connect one end of a CAT5 cable to a KVM port on the primary KVM/net.
 - b. Connect the other end of the CAT5 cable to a KVM Terminator.
 - c. Connect the Terminator's VGA and PS/2 connectors to the User 1 port on the secondary KVM, KVM/net, or KVM/net Plus.

See "Connecting Servers to the KVM Ports" on page 70 for detailed instructions on how to connect devices to KVM ports using KVM Terminators.
4. Repeat steps 1 through 3 for each secondary KVM to be connected to the primary KVM/net.

▼ **To Connect a KVM Expander to the Primary KVM/net**

See “Installing the AlterPath KVM Expander” on page 108 for background information on the KVM Expander.

1. Power off all KVM hardware and connected devices.
2. Connect one end of a CAT5 cable to a KVM port on the primary KVM/net.
3. Connect the other end of the CAT5 cable to the User A and or the User B port on the secondary KVM Expander.

Note: To enable two concurrent KVM connections to ports on the KVM Expander, connect two CAT5 cables to two ports on the KVM/net. Connect one CAT5 cable to the User A port and the other CAT5 cable to the User B port on the KVM Expander.

4. Repeat steps 1 through 3 for each secondary KVM Expander to be connected to the primary KVM/net.

Installing the AlterPath KVM Remote Presence

With a CAT5 cable up to 500 feet long, the AlterPath KVM RP can be connected to the User 2 port of the KVM/net unit, enabling the extended user to perform local administration tasks or to select the local keyboard, video, and mouse console between a local station and a server connected to the KVM/net.

Tasks	Where Documented/Notes
1 Place the RP on a desk or table up to 500 feet away from the KVM/net.	You can use a CAT5 cable of up to 500 feet long to extend the local administration of the KVM/net.
2 Connect the RP to the KVM/net.	“To Connect the RP to the KVM/net” on page 120.
3 Connect a keyboard, monitor, and mouse to the RP.	“Options for Accessing the RP” on page 120
4 Supply power to and turn on the RP.	“Supplying Power to the RP” on page 121
5 Use the RP to control the KVM/net.	“Controlling the OSD Through the AlterPath Remote Presence” on page 387

Shipping Box Contents KVM RP

The shipping box for the KVM RP contains the KVM RP along with the items shown in Table 3-2. The entry for each part provides an illustration, its part number (P/N), description, and purpose. You can use check boxes to check off each item, and you can use the part numbers from this table to reorder any of the parts.

Table 3-2: KVM RP Shipping Box Contents, Part Numbers, and Description (Sheet 1 of 2)


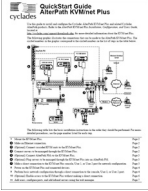


<input checked="" type="checkbox"/>	Item	P/N	Description	Purpose
<input type="checkbox"/>		PAC0226	Documentation CD	PDF copies of this guide and all other Cyclades product documents.
<input type="checkbox"/>		PAC0303	<i>AlterPath KVM/net Quick Start Guide</i>	Basic installation guide for experienced users in printed format.
<input type="checkbox"/>		CAB0010	3-pin power cord	Use to plug into a grounded AC power outlet. For other types of power sources, contact Cyclades sales for other cord options.
<input type="checkbox"/>		CAB0018	RJ-45 to RJ-45 7ft. CAT5 cable	Use to connect the User 2 port on the KVM/net to the Remote User port on the KVM RP. See “To Connect the RP to the KVM/net” on page 120.

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

<input checked="" type="checkbox"/>	Item	P/N	Description	Purpose
<input type="checkbox"/>		ATP4710	KVM cable	Use to connect the VGA port, PS/2 keyboard port, and PS/2 mouse port on the back of your PC to the PC VGA port, PS/2 keyboard port, and PS/2 mouse port on the RP. See “To Connect the RP to the Local Work Station” on page 121 more information.

▼ **To Connect the RP to the KVM/net**

1. Put one end of a CAT5 cable into the Remote User port on the KVM RP.
2. Put the other end of the CAT5 cable into the User 2 port on the KVM/net.

Options for Accessing the RP

The RP offers the two options for monitor, keyboard, and mouse control. Administrators can connect a dedicated keyboard, monitor, and mouse directly to the RP. Or administrators can connect the RP to their local work station in order to toggle the keyboard, monitor, and mouse control between the KVM/net and the local computer.

▼ **To Connect the RP to a Dedicated Keyboard, Monitor, and Mouse**

1. Connect your monitor’s VGA cable to the USER VGA port on the RP.
2. Connect your keyboard’s PS/2 cord to the USER keyboard PS/2 port on the RP.
3. Connect your mouse’s PS/2 cord to the USER mouse PS/2 port on the RP.

▼ **To Connect the RP to the Local Work Station**

1. Connect your monitor's VGA cable to the PC VGA port on the RP.
2. Connect your keyboard's PS/2 cord to the PC keyboard PS/2 port on the RP.
3. Connect your mouse's PS/2 cord to the PC mouse PS/2 port on the RP.
4. Use a KVM cable to connect the VGA port, PS/2 keyboard port, and PS/2 mouse port on the back of your PC to the PC VGA port, PS/2 keyboard port, and PS/2 mouse port on the RP.

Note: When the RP is connected to the local PC, as described in the previous procedure, the RP receives power from the PC and does not need to be plugged into a power supply.

Supplying Power to the RP

The RP can be powered by a power cord connected to its power supply port, or it can be powered by the local work station. Power can be transmitted from the PC through a KVM cable to the RP.

▼ **To Power On the KVM RP**

1. If the RP has its own dedicated keyboard, monitor, and mouse connected to its USER port, do the following:
 - a. Make sure the KVM/net's power switch is off.
 - b. Plug in the power cable.
 - c. Turn the KVM/net's power switch on.
2. If the RP is connected to the local PC, turn the KVM/net's power switch on.

The power is supplied by the PC. See "To Connect the RP to the Local Work Station" on page 121 for instructions on connecting the RP to the local PC.

Installing KVM/net-related Products and Components

Chapter 4

Web Manager for Administrators

This chapter is for administrators who use the Web Manager for managing and configuring the KVM/net. Two types of administrators can access all the Web Manager functions described in this chapter:

- An administrator who knows the password for the “admin” account, which is configured by default
- An optionally-configured regular user whose account is in the “admin” group (See “Users & Groups” on page 175 for how the admin adds a regular user account and adds the account to the admin group.)

Administrators whose accounts are configured without administrative access can log into the Web Manager as regular users and then access connected devices, as described in Chapter 5. “Web Manager for Regular Users” on page 267. For more background about the differences between user types, see “Types of Users” on page 16.

Before following the procedures in this chapter, review “Prerequisites for Using the Web Manager” on page 22, if needed, to make sure that you can connect to the Web Manager.

The sections listed in the following table give background information related to KVM/net administrators’ use of the Web Manager, including explanations of the types of information to be entered in each of the forms, and links to all the procedures performed in each mode.

Common Features of Administrators’ Windows	Page 126
Logging Into the Web Manager and Saving Changes	Page 128
Administrative Modes	Page 131
Wizard Mode	Page 131
Expert Mode	Page 141

Common Tasks

The following table lists common tasks that KVM/net administrators perform with links to the procedures.

Task	Where Documented/Notes
Set up other users to access connected devices without being able to make changes to the KVM/net configuration	<ul style="list-style-type: none">• “To Add a User [Wizard]” on page 135• “To Add a User [Expert]” on page 176
Assign users or groups to specific ports, restricting access to a limited set of devices	<ul style="list-style-type: none">• “To Assign KVM Port Access to a User or Group” on page 180
Set up other users to share all administration of the KVM/net	<ul style="list-style-type: none">• “To Add a User [Wizard]” on page 135• “To Add a User [Expert]” on page 176
Enable direct login to ports from the Web Manager login screen	<ul style="list-style-type: none">• To Enable Direct Access to KVM Ports [Expert]
Set up logging of system messages to a syslog server	<ul style="list-style-type: none">• “To Add a Syslog Server [Wizard]” on page 140• To Delete a Syslog Server [Wizard]• To Configure Syslogging for KVM Ports and Specify Message Filtering [Expert]• To Configure Creation of Alarms and Syslog Files for IPDUs [Expert]

Task	Where Documented/Notes
Configure power management for one or both of the AUX ports (if the port is connected to an optional AlterPath PM or other supported IPDU device)	<ul style="list-style-type: none"> • “To Configure the AUX Port for Use With a PM or an External Modem” on page 240 <p>Also see the procedures under “Power Management” on page 144 including:</p> <ul style="list-style-type: none"> • “To View Status, Lock, Unlock, and Cycle Power Outlets [Expert]” on page 146 • “To View and Reset IPDU Information [Expert]” on page 147 • “To Configure Creation of Alarms and Syslog Files for IPDUs [Expert]” on page 150 • “To Upgrade Firmware on an AlterPath PM [Expert]” on page 151
Choose among authentication methods and specify authentication servers for logins to the KVM/net and for logins to devices connected to the KVM/net’s ports	<ul style="list-style-type: none"> • “To Configure an Authentication Method for KVM/net Logins” on page 186 • “To Configure an Authentication Method for Logins Through KVM Ports” on page 187
Specify encryption levels for KVM ports	“To Configure Encryption on Port Connections [Expert]” on page 184
Configure rules for the KVM/net to filter packets like a firewall	<ul style="list-style-type: none"> • “To Add a Chain for IP Filtering” on page 220 • “To Edit A Chain for IP Filtering” on page 222 • “To Add a Rule for IP Filtering” on page 222 • “To Edit a Rule for IP Filtering” on page 219

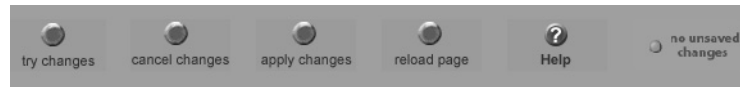
Common Features of Administrators' Windows

The features of all Web Manager windows for KVM/net administrators are described in the following sections:


- Control and logout buttons and KVM/net Information
See “Administrators’ Control Buttons, Logout Button, and KVM/net Information.”
- Getting more information
See “Obtaining More Information” on page 127


Administrators’ Control Buttons, Logout Button, and KVM/net Information

The following figure shows the control buttons that display at the bottom of the window when the logged in user is an administrator.





The following table describes the uses for each control button.

Button Name	Use
try changes	Tests the changes entered on the current form without saving them.
cancel changes	Cancels all unsaved changes.
apply changes	Applies all unsaved changes.
reload page	Reloads the page.
Help	Brings up the online help with information relating to the current form.
	The unsaved changes button appears on the lower right hand corner of the Web Manager and a graphical LED blinks red whenever the current user has made any changes and has not yet saved the changes.

Button Name	Use
	The no unsaved changes button appears and a graphical LED appears in green when no changes have been made that need to be saved.

The following table describes the logout button and the other information that displays in the upper right corner of all Web Manager windows.

Window Area	Purpose
	Click this button to log out.
	Displays the hostname and IP address assigned during initial configuration (see “Performing Basic Network Configuration” on page 76). Also displays the model name of the KVM/net.

Obtaining More Information

Information about the purpose of each Web Manager form and the values to be specified on the form is available by clicking the Help button. For definitions of unfamiliar terms see the Glossary. For links to sections of the book where unfamiliar terms are discussed, see the Index.

Logging Into the Web Manager and Saving Changes

The following table lists procedures common to both Wizard and Expert mode.

To Log Into the Web Manager as Admin	Page 128
To Save Configuration Changes	Page 128

For procedures specific to each mode, see “Administrative Modes” on page 131.

▼ *To Log Into the Web Manager as Admin*

This procedure assumes that the prerequisites described under “Prerequisites for Using the Web Manager” on page 22 are done and that you can connect to the Web Manager.

1. To bring up the Web Manager, enter the IP address of the KVM/net in the address (URL) field of a supported browser on a computer running a Windows operating system.

Note: Devices like the KVM/net V1 that are installed in computer rooms are usually assigned fixed IP addresses. If DHCP is enabled, you must find out the dynamically-assigned IP address each time before you bring up the Web Manager. Check with the administrator who configured the basic network parameters on the KVM/net, for help finding the IP address, if needed. Or see “Considerations When Choosing Whether to Enable DHCP” on page 50 for a list of ways to find out the KVM/net IP address assigned by the DHCP server.

- a. If DHCP is enabled, enter the dynamically-assigned IP address.
- b. If DHCP is not enabled, use a fixed IP address assigned by the administrator to the KVM/net.

The Login page appears. If direct logins to ports is not enabled, a “username” and a “password” field appear on the login area of the screen, as shown in the following screen example.

Logging Into the Web Manager and Saving Changes



If direct logins to KVM ports is enabled, a “port” field also appears in the login area of the screen, as shown in the following screen example.



2. If direct logins to ports is enabled, to bring up the Web Manager with the port number filled in, enter the IP address of the KVM/net followed by the port number in the form.

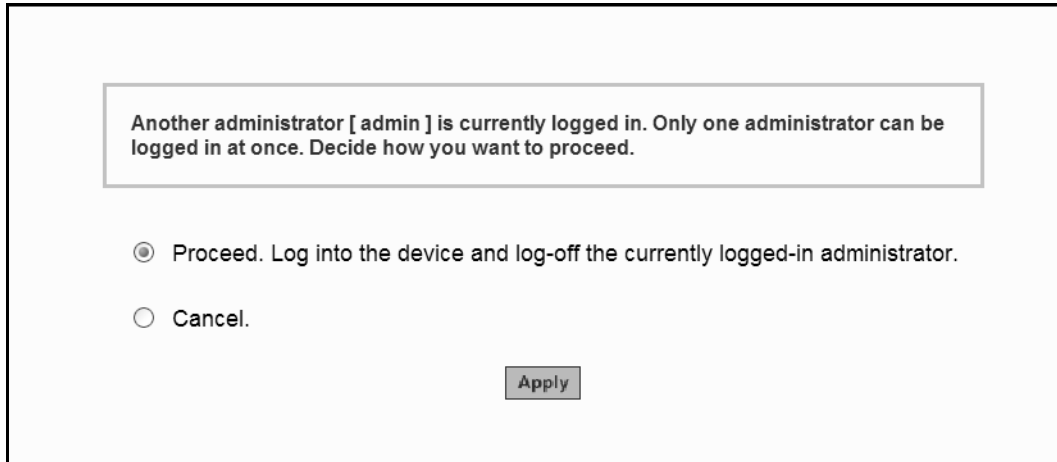
```
IP_address/login.asp?portname=portnumber
```

A login screen displays empty “username” and “password” fields and a port field filled with the name of the port from the URL you entered in the browser.

See “Web Manager Login Screen” on page 281 for background information on the multiple ways to login to the Web Manager.

3. Enter your account's username and password.

If another administrator is already logged in as "admin," the dialog box shown in the following screen example appears.



The screenshot shows a dialog box with a title bar and a message: "Another administrator [admin] is currently logged in. Only one administrator can be logged in at once. Decide how you want to proceed." Below the message are two radio buttons: "Proceed. Log into the device and log-off the currently logged-in administrator." (which is selected) and "Cancel." At the bottom center is an "Apply" button.

Note: For more information about the numbers of simultaneous logins allowed, see "Simultaneous KVM/net Logins" on page 17.

If the previous dialog box appears, go to [Step 4](#).

4. Click the appropriate radio button and then click Apply.

▼ **To Save Configuration Changes**

The red graphical LED in the lower right hand corner of the Web Manager blinks when any changes made in the forms have not been saved.

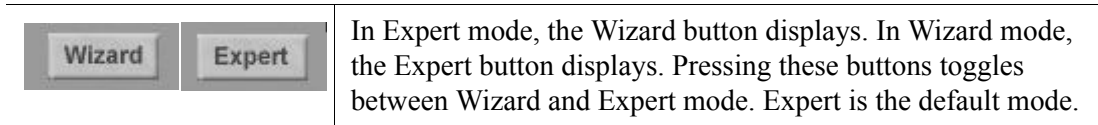
- Click the "apply changes" button to save configuration changes.

The "no unsaved changes" graphical LED appears.

Administrative Modes

This section describes the two administrative modes of the web manager:

- “Wizard Mode” on page 131
- “Expert Mode” on page 141



Wizard Mode

The Wizard mode guides the administrator through three configuration steps. The following figure shows a typical window in Wizard mode. Selecting an item from the left menu brings up a corresponding form in the middle.

After you log in as described in “To Log Into the Web Manager as Admin” on page 128, Expert mode is in effect by default. To change to Wizard mode, select the Wizard button, which displays only in Expert mode.

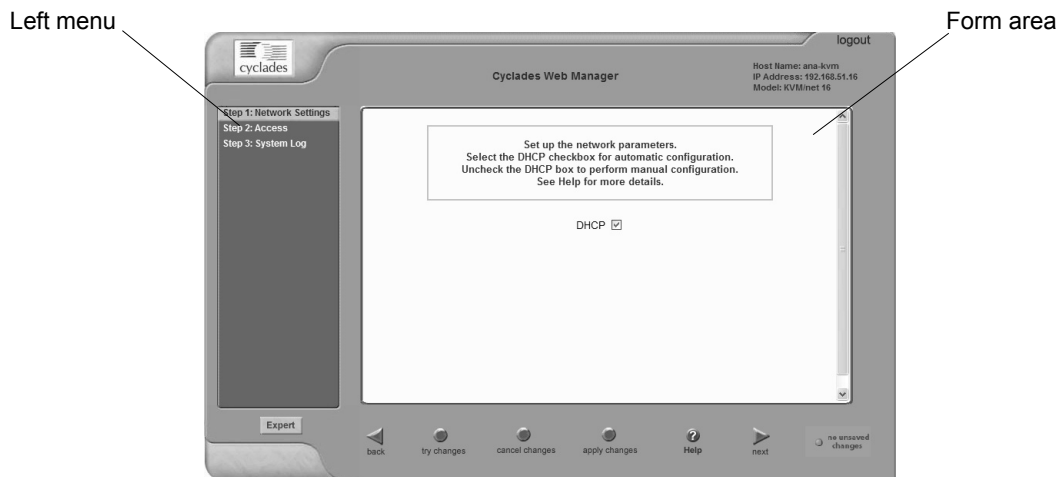


Figure 4-1: Example Window in Wizard Mode

Procedures in Wizard Mode

The following table lists all procedures that are performed in Wizard mode.

To Change Network Settings [Wizard]	Page 133
To Add a User [Wizard]	Page 135
To Delete a User [Wizard]	Page 137
To Change a Password [Wizard]	Page 137
To Add a Syslog Server [Wizard]	Page 140
To Delete a Syslog Server [Wizard]	Page 140

Steps in Wizard Mode

Three configuration steps display in the left menu of the Web Manager in Wizard mode. The following table lists the sections where the steps are described.

Step 1: Network Settings [Wizard]	Page 132
Step 2: Access [Wizard]	Page 134
Step 3: System Log [Wizard]	Page 139

Step 1: Network Settings [Wizard]

In Wizard Mode, selecting "Step 1: Network Settings" brings up a form for reconfiguring existing network settings. During initial setup of the KVM/net, the administrator configures the default basic network settings that were needed to enable logins through the Web Manager. (See "Performing Basic Network Configuration" on page 87, if desired, for more information about the initial network configuration.) You can skip this step if the current settings are correct. Check with your network administrator if you are not sure.

Before making any changes to existing network settings, you may want to review "Collecting Basic Network Information" on page 84, which provides a form to record information you need to collect ahead of time. See "To Change Network Settings [Wizard]" on page 133 for the procedure.

In Expert mode, under Configuration>Network, you can specify additional networking-related information: a Console Banner, a secondary IP address and secondary network mask, and an MTU. See “To Configure Host Settings [Expert]” on page 205. In Expert mode under Configuration>Network, you can configure syslog servers for ports; specify rules for filtering syslog messages, specify PCMCIA card, Virtual Private Network (VPN), and SNMP settings; specify IP filtering rules (for the KVM/net to act as a firewall), and perform other advanced configuration tasks.

▼ To Change Network Settings [Wizard]

1. Collect any IP addresses or other network information to change.

See the list of network information to collect under “Performing Basic Network Configuration” on page 76, if needed.

2. In Wizard mode, go to “Step 1: Network Settings.”

If the “DHCP” check box is not checked, the DHCP selection page displays as shown below. If the “DHCP” check box is checked, only the check box appears below the instructions.

Note: If DHCP is enabled, a local DHCP server assigns the KVM/net a dynamic IP address that can change. The administrator chooses whether or not to use DHCP during initial setup. The initial setting may have been changed since initial configuration.

3. If the “DHCP” check box is not checked, enter the network information in the fields.

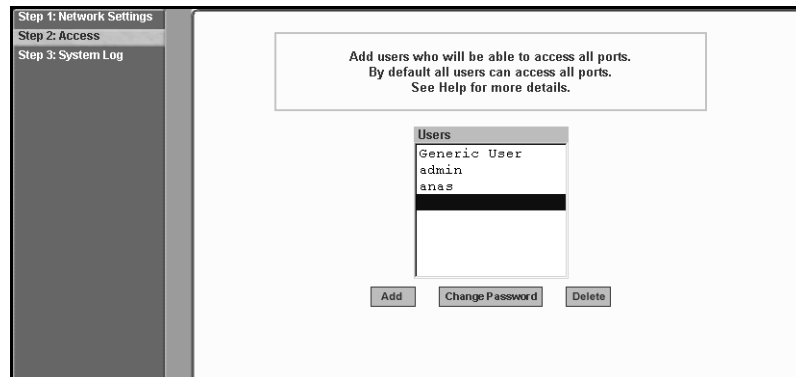
4. Click the “apply changes” button.

Warning! If you change the KVM/net’s IP address and apply the changes, you will need to reconnect to the Web Manager with the new IP address.

5. If appropriate, press the Next button or select “Step 2: Access” from the left menu.

Step 2: Access [Wizard]

In Wizard mode, selecting “Step 3: Access” brings up a form for adding or deleting users and for setting or changing passwords. Use this form if you want to add user accounts to allow other administrators to administer connected devices without being able to change the configuration of the KVM/net. Added users can optionally be configured to administer the KVM/net by assigning them to the “admin” group.



The Access form lists the currently defined Users and has three buttons: Add, Change Password, and Delete.

In the Users list, by default, are two user accounts that cannot be deleted:

- Admin
- Generic User

The Admin (the “admin” account) has access to all functions of the Web Manager and has access to all ports on the KVM/net.

The Generic User defines the access permissions for all users except the admin and root users. Any new regular user account automatically inherits the access permissions configured for the Generic User.

The following lists has links to the procedures for adding and deleting regular users and changing the passwords for regular users or administrators.

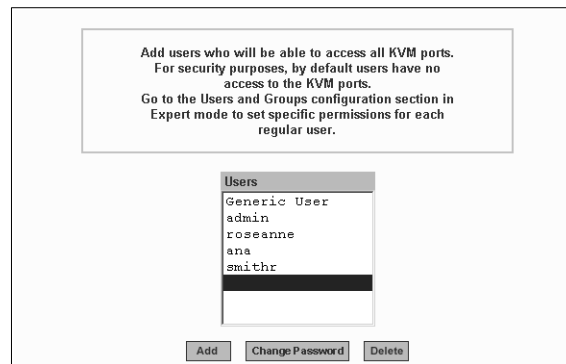
To Add a User [Wizard]	Page 135
To Delete a User [Wizard]	Page 137
To Change a Password [Wizard]	Page 137

Note: To perform advanced configuration for users and groups, for example, to restrict user access to KVM ports, or to create a group, go to Expert>Configuration >Users and Groups.

▼ **To Add a User [Wizard]**

1. In Wizard mode, go to Step 3: Access.

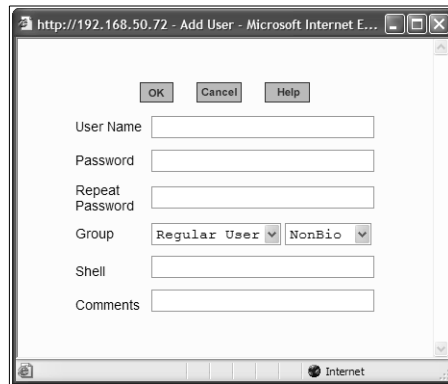
The Access form appears.



2. Click Add.

The “Add User” dialog box appears.

Web Manager for Administrators



The screenshot shows a web browser window titled "http://192.168.50.72 - Add User - Microsoft Internet E...". The form contains the following fields and controls:

- Buttons: OK, Cancel, Help
- User Name:
- Password:
- Repeat Password:
- Group:
- Shell:
- Comments:

3. Enter the required information in the fields as shown in the following table.

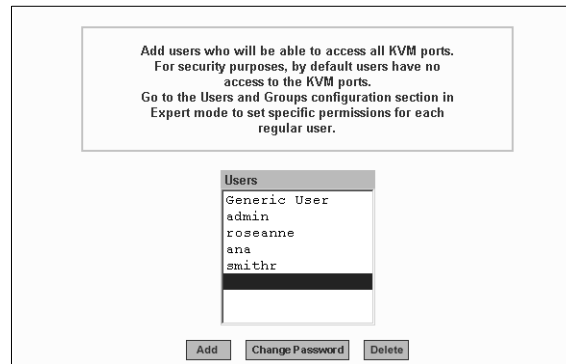
Field Name	Definition
User Name	The username for the account being added.
Password	The password for the account.
Group	On the pull-down menu, Select Regular User [Default] or Admin. Note: To configure a user to be able to perform all KVM/net administration functions, select the “Admin” group. See “Types of Users” on page 16, if needed, for more background.
Shell	Optional. The default shell when the user makes a <code>ssh</code> or <code>telnet</code> connection with the switch. Choices are: <code>sh</code> or <code>bash</code> . The default is <code>sh</code> .
Comments	Optional notes about the user’s role or configuration.

4. Click OK.
5. Click the “apply changes” button.

▼ **To Delete a User [Wizard]**

1. In Wizard mode, go to “Step 3: Access.”

The “Access” form displays.



1. Select the user name to delete.
2. Click “Delete.”

The username disappears from the Users list.

3. Click the “apply changes” button.

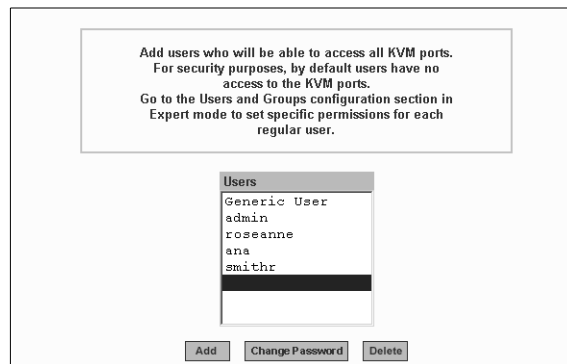
▼ **To Change a Password [Wizard]**

Note: Leaving the default admin or root passwords unchanged would leave the KVM/net and connected devices open to anyone who knows the default passwords and the KVM/net’s IP address. For security’s sake, make sure the admin and root passwords have been changed from the default “cyclades.” If either the admin or root passwords have not been changed, change them now.

1. In Wizard mode, go to “Step 3: Access.”

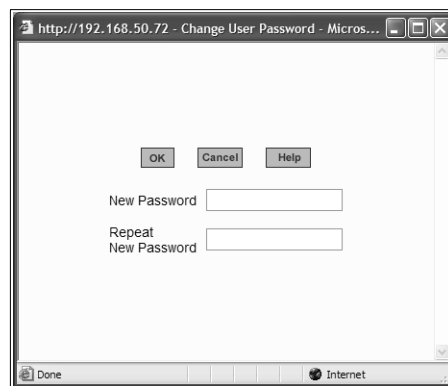
The “Access” form appears.

Web Manager for Administrators



2. Select the name of the user whose password you want to change.
3. Click “Change Password.”

The “Change User Password” dialog box appears.



4. Enter the new password in both fields, and click OK.
5. Click the “apply changes” button.

Step 3: System Log [Wizard]

In Wizard mode, selecting “Step 3: System Log” brings up a form for identifying one or more syslog servers to receive syslog messages from the KVM/net.

Before performing this procedure, make sure an already-configured syslog server is available to the KVM/net.

Obtain the following information from the syslog server’s administrator:

- The IP address of the syslog server
- The facility number for messages coming from the KVM/net

Each syslog server has eight local facility numbers (Local 0 through Local 7) that the syslog server’s administrator can assign and use for handling log messages from different locations. See “Syslog Servers” on page 49, if needed, for more background on logging and on how facility numbers are used.

The following table has links to the procedures for adding and deleting a syslog server.

To Add a Syslog Server [Wizard]	Page 140
To Delete a Syslog Server [Wizard]	Page 140

This form configures system logging for the KVM/net. More advanced configuration of syslog servers and event notification can be done in Expert mode. To configure system logging for messages relating to KVM ports, in

Expert mode go to “To Configure Syslogging for KVM Ports and Specify Message Filtering [Expert]” on page 208.

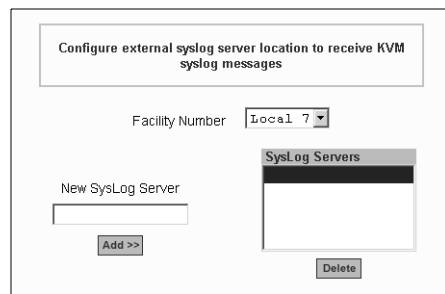
▼ **To Add a Syslog Server [Wizard]**

This procedure assumes you have the following information:

- The IP address of the syslog server
- The facility number for messages coming from the KVM/net

1. In Wizard mode, go to “Step 3: System Log.”

The System Log form appears.



The screenshot shows a web form titled "Configure external syslog server location to receive KVM syslog messages". It contains a "Facility Number" dropdown menu currently set to "Local 7". Below this is a "New SysLog Server" text input field with an "Add >>" button underneath. To the right is a "SysLog Servers" list box, which is currently empty, with a "Delete" button below it.

2. From the Facility Number drop-down menu, select the facility number.
3. In the New Syslog Server field, enter the IP address of a syslog server, and select the Add button. (Repeat this step until all syslog servers are listed.)
4. The new server(s) appear in the Syslog Servers list.
5. Click “apply changes.”

▼ **To Delete a Syslog Server [Wizard]**

1. From the Syslog Server list, select the syslog server that you want to delete from the current facility location, and select Delete.
2. Repeat this step for as many servers you need to delete.
3. Click “apply changes.”

Expert Mode

To perform advanced configuration, click the Expert button at the bottom of the left menu to switch to Expert mode. The following figure shows a typical window in Expert mode.



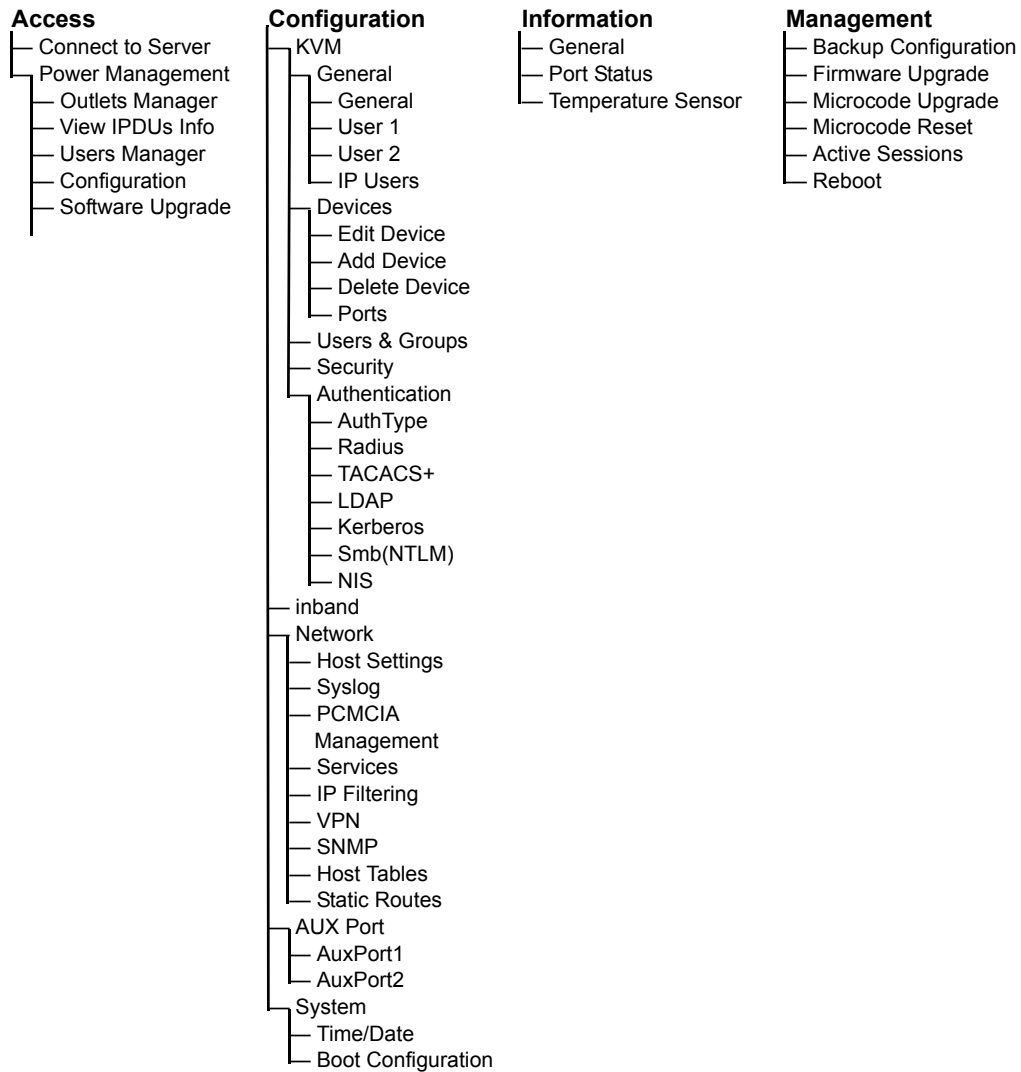
Making a selection from the top menu changes the list of menu options displayed in the left menu.

An option in the left menu (such as KVM in the preceding figure) often has several forms associated with it. Selecting a tab labeled with the name of the form or selecting the form's name in the left menu brings up the form.

Note: Procedures in this manual use shortcuts to tell how to get to Web Manager forms. For example, a step telling the user to access the “IP Users” form in the right tab in the previous figure would use this convention, “In Expert mode, go to Configuration> KVM>General >IP Users.”

Overview of Menus and Forms in Expert Mode

The following figure shows all the menus and forms available in Expert mode. If you are viewing this document online, click any term to go to the section where the form is described.



Access

Under “Access” in Expert mode, four options appear in the left menu bar, as shown in the following figure.



See the following sections for details about the tasks performed using the forms under Access in Expert mode.

- “Connect to Server” on page 143
- “Power Management” on page 144

For instructions for forms that allow the regular user to connect to ports on the KVM/net to administer connected devices and perform power management, see Chapter 5: Web Manager for Regular Users.

Connect to Server

On the “Connect to Server” form under Access, you can connect to servers that are connected to KVM ports or to in-band servers that use RDP (Remote

Web Manager for Administrators

Desktop Protocol). The following sections in Chapter 6: Accessing Connected Devices discusses connecting to servers in more detail:

- “Prerequisites for Accessing Servers With In-band Connections” on page 280
- “Prerequisites for Accessing Servers With KVM Connections” on page 281
- “Connecting to Servers Remotely Through the Web Manager” on page 286
- “Connecting to Servers Locally Through the OSD” on page 292
- “Sharing a Server Connection” on page 317
- “AlterPath Viewer Settings” on page 305

Power Management

On the “Power Management” forms under “Access” in Expert mode, you can manage power for devices that are plugged into the outlets on one or more intelligent power distribution units (IPDUs).

The screenshot displays the Cyclades Web Manager interface. The top navigation bar includes 'Access | Configuration | Information | Management' and a 'logout' link. The user's session information is shown as 'Host Name: ana-kvm', 'IP Address: 192.168.45.21', and 'Model: KVM/net 16'. The main content area is titled 'Outlets Manager' and contains a table with the following data:

Outlet	Outlet Name	Outlet State	Power Up Interval
1	out1	⚡ 🔒 Cycle	0.50
2	out2	⚡ 🔒 Cycle	0.50
3	out3	⚡ 🔒 Cycle	0.50
4	out4	⚡ 🔒 Cycle	0.50
5	out5	⚡ 🔒 Cycle	0.50
6	out6	⚡ 🔒 Cycle	0.50
7	out7	⚡ 🔒 Cycle	0.50
8	out8	⚡ 🔒 Cycle	0.50

The interface also features a sidebar with 'Connect to server' and 'Power Management' options, a 'Wizard' button, and a bottom navigation bar with buttons for 'try changes', 'cancel changes', 'apply changes', 'reload page', 'Help', and 'no unsaved changes'.

You can manage power when the following two prerequisites are completed:

- An AlterPath PM or other IPDU is connected to an AUX port on the KVM/net. The AlterPath PM can be daisy chained to allow you to manage power for up to 128 devices from the KVM/net.

For the procedure, see “To Connect a PM to the AUX Port” on page 106.

- The AUX port is configured for power management.

For the procedure, see “To Configure the AUX Port for Use With a PM or an External Modem” on page 240.

See the following sections for details about the tasks performed using the forms under Power Management.

- “Outlets Manager” on page 145
- “View IPDUs Info” on page 147
- “Users Manager” on page 148
- “Configuration” on page 149
- “Software Upgrade” on page 150

See the following sections for related procedures:

- “To View Status, Lock, Unlock, and Cycle Power Outlets [Expert]” on page 146
- “To View and Reset IPDU Information [Expert]” on page 147
- “To Configure Users to Manage Specific Power Outlets” on page 148
- “To Configure Creation of Alarms and Syslog Files for IPDUs [Expert]” on page 150
- “To Upgrade Firmware on an AlterPath PM [Expert]” on page 151

Outlets Manager

On the “Outlets Manager” form under Access>Power Management in Expert mode, you can do the following for all outlets on all connected IPDUs:

- Check the status
- Turn on
- Turn off
- Cycle (by briefly switching the outlet off and on)
- Lock
- Unlock

Outlets Manager		View IPDUs Info	Users Manager	Configuration	Software Upgrade
Device/Port: master/AUX					
Outlet	Outlet Name	Outlet State		Power Up Interval	
1	out1			Cycle	0.50
2	out2			Cycle	0.50
3	out3			Cycle	0.50
4	out4			Cycle	0.50
5	out5			Cycle	0.50
6	out6			Cycle	0.50
7	out7			Cycle	0.50
8	out8			Cycle	0.50

▼ **To View Status, Lock, Unlock, and Cycle Power Outlets [Expert]**

1. In Expert mode, go to Access>Power Manage IPDU>Outlets Manager.

The “Outlets Manager” form appears.

Yellow bulbs indicate an outlet is switched on and an opened padlock indicates that the outlets are unlocked. An orange “Cycle” button is active next to each outlet that is on.

2. To switch an outlet on or off, click the adjacent light bulb.
3. To lock or unlock an outlet, click the adjacent padlock.

In the example below, outlet 1 is switched on and locked, and outlet 2 is switched off and unlocked.

1	out1			Cycle	0.50
2	out2			Cycle	0.50

4. To power an outlet off and quickly power it on again, click the adjacent “Cycle” button.
5. Click “apply changes.”

View IPDUs Info

On the “View IPDUs Info” form under Access>Power Manage IPDU in Expert mode, you can view the following information about any connected IPDUs:

- Number of outlets on each unit
- Current
- Temperature
- Alarm threshold levels
- Firmware version

You can also clear values for the maximum current and the maximum temperature.

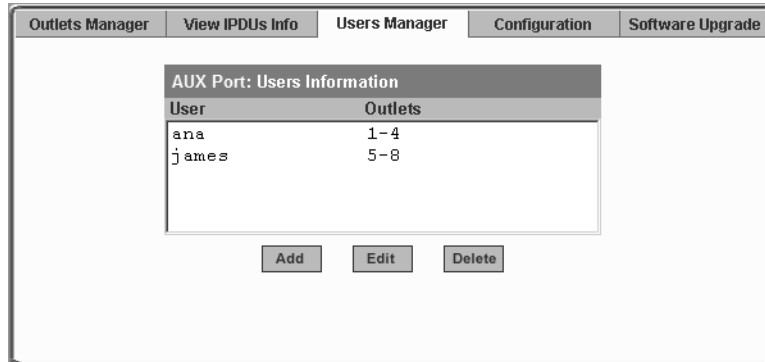
AUX Port: General Information		Clear Max Detected Current	Clear Max Detected Temperature
Name: PowerMgm-1	Syslog: ON	Number of Outlets: 8	
Number of Units: 1	Buzzer: ON	Over Current Protection: OFF	
Master Unit Information:			
Model: PM8 20A		Software Version: 1.5.0	
Alarm Threshold: 20.0A		Maximum Detected: 1.3A	
Current: 0.0A		Maximum Detected:	
Temperature:			

▼ **To View and Reset IPDU Information [Expert]**

1. In Expert mode, go to Access>Power Management>View IPDUs Info.
The “View IPDUs Info” form appears.
2. To clear the stored values for the maximum detected current, select the “Clear Max Detected Current” button.
3. To clear the stored values for the maximum detected temperature, click the “Clear Max Detected Temperature” button.
4. Click “apply changes.”

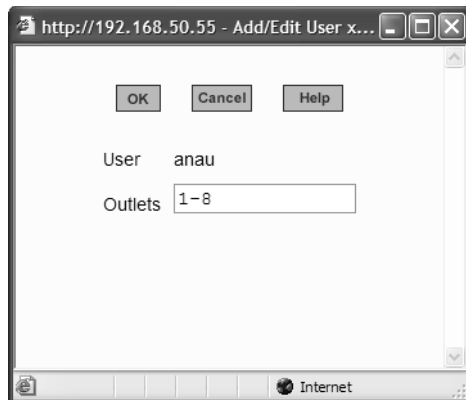
Users Manager

On the “Users Manager” form under Access>Power Management in Expert mode, you can assign users to outlets.



▼ ***To Configure Users to Manage Specific Power Outlets***

1. In Expert mode, go to Access>Power Management>Users Manager.
The “Users Manager” form appears.
2. To remove a user’s ability to manage power, select the username and click “Delete.”
3. To edit a user, select the username from the view table and click “Edit.”
Skip to [Step 5](#)..
The “Add/Edit User x Outlets” dialog box appears.



4. To add a new user, click “Add.”

The “Add/Edit User x Outlets” dialog box appears.

5. In the “Add/Edit User x Outlets” dialog box, do the following as appropriate.
 - a. Enter the username in the “User” field.
 - b. Enter or modify the numbers of the outlets to which the user is assigned in the “Outlets” field.

Use a comma to separate outlet numbers, and use a hyphen to indicate a range of outlets (for example: 1, 3, 6, 9-12).

6. Click OK.
7. Click “apply changes.”

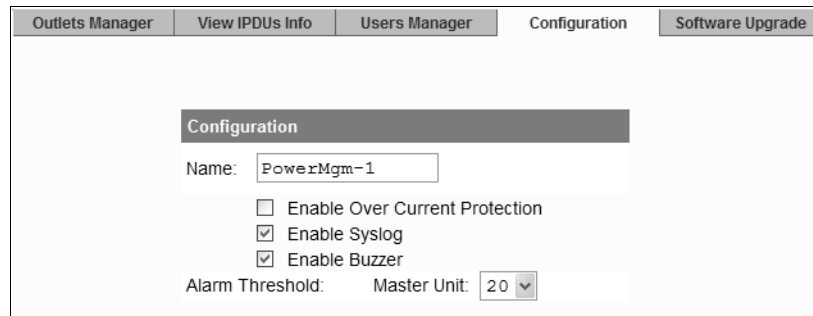
Configuration

On the “Configuration” form under Access>Power Management in Expert mode, you can specify the following:

- Whether syslog messages are generated for power management events
- Over current protection:
 - An alarm threshold
 - Whether a buzzer sounds whenever the current exceeds the defined threshold.

You can define the alarm threshold for both a master and a slave unit.

The Configuration form shows the ports that are currently connected to IPDUs. The following example displays for an KVM/net with an AlterPath PM connected to AUX port.



The screenshot shows a web interface with a navigation bar at the top containing five tabs: 'Outlets Manager', 'View IPDUs Info', 'Users Manager', 'Configuration', and 'Software Upgrade'. The 'Configuration' tab is active. Below the navigation bar is a form titled 'Configuration'. The form has a 'Name' field containing 'PowerMgm-1'. Below the name field are three checkboxes: 'Enable Over Current Protection' (unchecked), 'Enable Syslog' (checked), and 'Enable Buzzer' (checked). At the bottom of the form, there are two pull-down menus: 'Alarm Threshold' and 'Master Unit', with the 'Master Unit' menu currently showing '20'.

▼ **To Configure Creation of Alarms and Syslog Files for IPDUs [Expert]**

1. In Expert mode, go to Access>Power Management>Configuration.
The Configuration form displays entries for all ports configured for power management.
2. Click the appropriate check boxes to enable or disable Over Current Protection, the generation of Syslog files, and the sounding of a Buzzer if a defined threshold is exceeded.
3. If enabling the buzzer or alarm notification, select an Alarm Threshold (1-20 amps) from the pull-down menu for the master and any slave unit.
4. Click “apply changes.”

Software Upgrade

On the “Outlets Manager” form under Access>Power Management in Expert mode, you can upgrade the Power Management firmware for AlterPath PM IPDUs.

Outlets Manager	View IPDUs Info	Users Manager	Configuration	Software Upgrade						
Latest software version available: <input type="button" value="Refresh"/>										
<table border="1"> <tr> <td>Name: PowerMgm-1</td> <td>Number of Units: 1</td> </tr> <tr> <td colspan="2">Master Unit:</td> </tr> <tr> <td colspan="2">Software Version: 1.5.0</td> </tr> </table>					Name: PowerMgm-1	Number of Units: 1	Master Unit:		Software Version: 1.5.0	
Name: PowerMgm-1	Number of Units: 1									
Master Unit:										
Software Version: 1.5.0										

An entry appears for every connected PM and for each slave. The version of the currently-installed firmware displays on the form. If the KVM/net has access to the Internet, clicking the Refresh button checks for a more-recent version of the PM firmware at the Cyclades website.

If the KVM/net does not have access to the Internet, upgrade is possible only if you first download a more-recent version of the PM firmware onto the KVM/net.

▼ **To Upgrade Firmware on an AlterPath PM [Expert]**

Perform this procedure if the firmware on a connected AlterPath PM unit is older than the most-recent firmware available at Cyclades, Corp.

This procedure requires one of the two following prerequisites to succeed:

- The KVM/net has access to the Internet so that it can automatically download the PM firmware from the Cyclades FTP server.

OR

- An Update button appears on the form.

An Update button appears on the Access>Power Management>Software Upgrade form if a copy of a more-recent version of the AlterPath PM firmware exists in the KVM/net's /tmp directory under the filename: /tmp/pmfirmware.

Web Manager for Administrators

- 1.** If the KVM/net can contact the Cyclades FTP server, and if a more recent version of the firmware is available at Cyclades, download the updated firmware onto the KVM/net.
 - a. Download the firmware onto a computer with a direct connection to the KVM/net.
 - b. Copy the firmware file to the KVM/net and put it in:
/tmp/pmfirmware.
- 2.** In Expert mode, go to Access>Power Management>Software Upgrade.
The Software Upgrade form displays.
- 3.** If the KVM/net has access to the Internet, click the Refresh button.
The KVM/net contacts the Cyclades website to check if a more recent version of the PM firmware is available. If a more recent version is available, the KVM/net downloads it from Cyclades and installs it on the PM.
- 4.** Click “Update.”
- 5.** Click “apply changes.”

Configuration

Under “Configuration” in Expert mode, four main options appear in the left menu, as shown in the following figure.

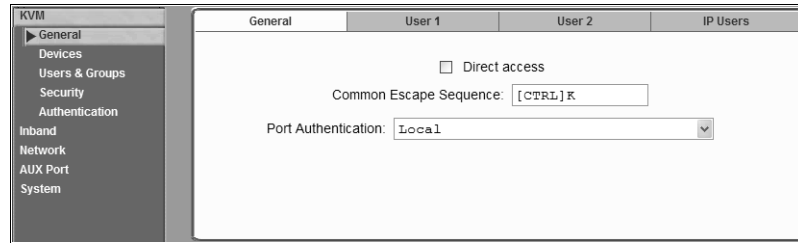


See the following sections for details about the tasks performed using the forms under Configuration in Expert mode:

- “KVM” on page 154
- “Configuring In-band (RDP) Servers” on page 197
- “Network” on page 203
- “AUX Port” on page 239
- “System” on page 241

KVM

Selecting Configuration>KVM in Expert mode brings up three KVM options in the left menu as shown in the following figure.

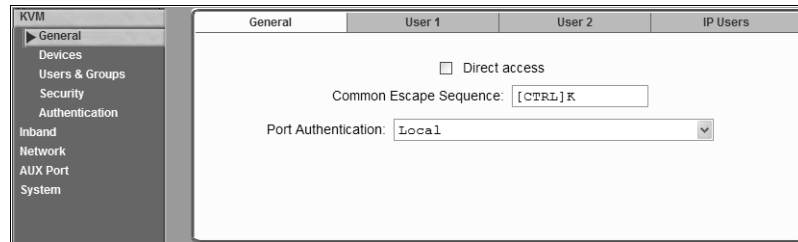


You can use the following KVM menu options for custom configuration of KVM ports. The following table provides links to the sections where the options are described.

General	Page 154
Modifying Individual KVM Ports	Page 164
Modifying Individual KVM Ports	Page 164
Security	Page 183

General

Selecting Configuration>KVM>General in Expert mode brings up three tabs, as shown in the following figure.



The following table provides links to the sections that describe how to use the forms under Configuration>KVM>General in Expert mode.

General	“General” on page 155.
---------	------------------------

User 1, “Local User and IP Users” on page 159
 User 2,
 and IP
 Users

General

On the General form under Configuration>KVM>General in Expert mode, you can specify the parameters shown in the following table.

Parameter Name	Definition	Where Documented
Direct Access	Selecting this check box enables logins to KVM ports directly from the Web Manager Login screen.	<ul style="list-style-type: none"> • “Enabling Direct Access to KVM Ports [Expert]” on page 193 • “To Enable Direct Access to KVM Ports [Expert]” on page 180
Common Escape Sequence	Redefines keyboard shortcuts used in the AlterPath Viewer	<ul style="list-style-type: none"> • “Redefining KVM AlterPath Viewer Keyboard Shortcuts (Hot Keys)” on page 180 • “To Redefine KVM Session Keyboard Shortcuts [Expert]” on page 181
Authentication Type	Allows you to choose whether authentication is required for KVM port logins. If needed, see the introduction to authentication on the KVM/net under “Authentication” on page 26.	<ul style="list-style-type: none"> • “Specifying Authentication for KVM Port Logins” on page 182 • “To Specify an Authentication Method for KVM Port Logins [Expert]” on page 182

Enabling Direct Access to KVM Ports [Expert]

When direct access to KVM ports is enabled, users authorized to access KVM ports can use a port field on the Web Manager login screen to log in and connect directly to the port. See “To Log Into the Web Manager as admin” on page 108, if desired, for an example of the login screen when direct login is enabled.

▼ To Enable Direct Access to KVM Ports [Expert]

1. Go to Configuration>KVM>General in Expert mode.
The General form appears.
2. Select the “Direct access” check box.
3. Click “apply changes.”

Redefining KVM Connection Keyboard Shortcuts (Hot Keys)

You can use the four General forms (General, User 1, User 2, IP Users) to redefine a default set of keyboard shortcuts (called hot keys), which allow administrators to perform common actions while connected to KVM ports. You redefine the common escape sequence portion of each hot key separately from the command key.

The following table summarizes the format of the hot keys for KVM connections, the defaults, and where they can be redefined.

	Common Escape Sequence	Command Key	Where Defined
Format	“Ctrl” + “ <i>letter key</i> ”	“ <i>letter key</i> ”	• Configuration>KVM>General> General

	Common Escape Sequence	Command Key	Where Defined
Defaults	Ctrl+k	“p” to bring up the “power management” window, “q” to quit, and so forth. See Table 6-3, “Default KVM Connection Keyboard Shortcuts,” on page 295 for all the default command keys.	<ul style="list-style-type: none"> • Configuration>KVM>General>User 1 • Configuration>KVM>General>User 2 • Configuration>KVM>General>IP Users

The following table has links to procedures for redefining the hot keys for KVM connections.

To Redefine KVM Session Keyboard Shortcuts [Expert].	Page 157
To Redefine KVM Session Keyboard Shortcuts [OSD] unresolved	Page 194

▼ **To Redefine KVM Session Keyboard Shortcuts [Expert]**

1. Go to Configuration>KVM>General in Expert mode.
The General form appears.
2. To redefine the “Common Escape Sequence” enter a key combination starting with the Ctrl key and followed by a letter, for example, **Ctrl m**.
3. To redefine the command key portion of any KVM-session keyboard shortcuts, do one of the following steps.
 - To change the command key for administrators who access KVM ports through the User 1 port, go to the User 1 tab.
 - OR -
 - To change the command key for administrators who access KVM ports through the User 2, go to the User 2 tab.
 - OR -

- To change the command key for users who access KVM ports through the Web Manager, go to the IP Users tab.
- 4. On the “User 1,” “User 2,” or “IP Users” tab, redefine the command keys, if desired, in any of the following fields: “Quit,” “Power Management,” “Mouse/Keyboard Reset,” “Video Control,” “Switch Next,” “Switch Previous,” “Port Info.”
- 5. Click “apply changes.”

Specifying Authentication for KVM Port Logins

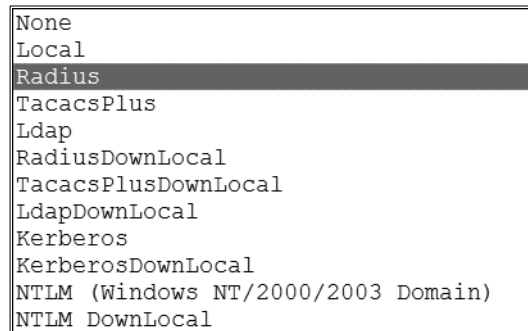
Choice of authentication types for KVM ports are:

- None
- Local
- Kerberos (either Kerberos or Kerberos/DownLocal),
- LDAP (either LDAP or LDAP/DownLocal)
- NTLM (either NTLM Windows NT/2000/2003 or NTLM/DownLocal)
- RADIUS (either RADIUS or RADIUS/DownLocal)
- TACACS+ (either TACACS+, and TACACS+/DownLocal)

▼ *To Specify an Authentication Method for KVM Port Logins*

This procedure configures a single authentication method that applies whenever anyone attempts to log into a device through a connected KVM port.

1. Go to Configuration>KVM>General in Expert mode.
The General form appears.
2. Select an authentication method from the Authentication pull-down menu.
The default option is None.



3. Click “Done.”
4. Click “apply changes.”

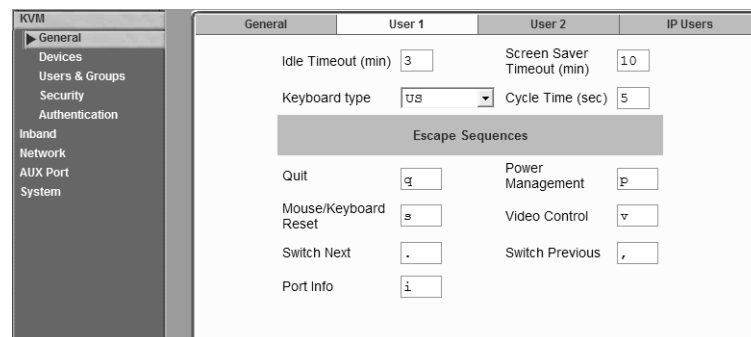
The changes are stored in `/etc/kvmd.conf` on the KVM/net.

5. If you select any authentication method other than None or Local, make sure that an authentication server is specified for the selected authentication type.

See “Configuring Authentication Servers for Logins to the KVM/net and Connected Devices” on page 160.

Local User and IP Users

Selecting Configuration>KVM>General>User 1 brings up a form with the fields shown in the following figure.



On the “User 1” form under Configuration>KVM>General in Expert mode you can redefine the default session parameters that apply when a user (called the *Local User*) is using the OSD through a direct connection to the KVM User 2 management port on the KVM/net. On the “User 2” form, you can

Web Manager for Administrators

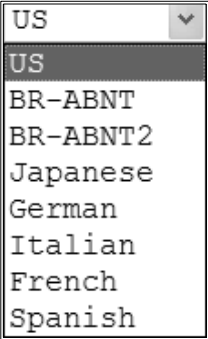
redefine the default session parameters that apply when a user is using the OSD through a KVM RP connection to the User 2 port on the KVM/net.

Selecting Configuration>KVM>General>IP Users brings up a form with the fields shown in the following figure.

On the “IP Users” form under Configuration>KVM>General in Expert mode, you can define the default session parameters that apply when a remote user (called the *IP User*) is connected to a KVM port through the Web Manager (in a type of session called *KVM over IP*).

The following table lists and describes the parameters that appear on the forms for both types of users.

Field Name	Definition
Idle Timeout	Sets the maximum time (in minutes) for the session to be idle before it is closed. The maximum value is 60 minutes. A value of 0 disables the idle timeout.
Screen Save Timeout	Sets the time (in minutes) for the session to be idle before the screen saver activates. The maximum value is 60 minutes. A value of 0 disables the idle timeout. [User 1 and User 2 only.]

Field Name	Definition
Keyboard Type	<p>Sets the keyboard type. [User 1 and User 2 only.] Choose the type of keyboard connected to the User 1 and User 2 ports on the KVM/net. The options from the drop-down list are shown in the figure.</p> 
Cycle Time	<p>Change the cycle time (in seconds) within the following range: 3 to 60 seconds. [User 1 and User 2 only.]</p>
TCP Viewer Ports	<p>Change the number of the TCP port used for the AlterPath Viewer. [IP Users only.] The default is 5900+. You may need to change the default, for example, if your firewall is blocking port 5900. (For more details, see “Port Numbers and Aliases” on page 23.) Port numbers 1-1024 are reserved. Indicate a range of ports by entering a plus sign (+) after the first port number (as in 2500+) or by entering a dash between two port numbers (as in 2500-2501). Indicate a set of nonadjacent port numbers by separating port numbers with commas (as in 2500, 2508).</p>

On the “User 1” and “User 2” and “IP Users” forms, you can also redefine the command key portion of keyboard shortcuts for each type of user. For more information about redefining keyboard shortcuts, see “Redefining Keyboard Shortcuts (Hot Keys)” on page 56 and “To Redefine KVM Session Keyboard Shortcuts [Expert]” on page 157 if needed.

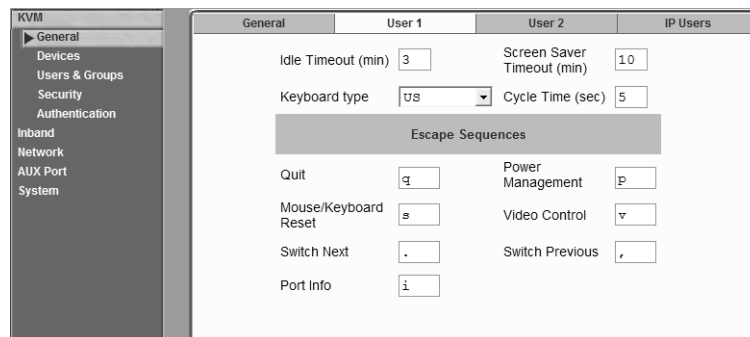
The following table shows procedures you can perform using the Local User or IP Users forms.

To Configure IP User (KVM Over IP) Sessions [Expert]	Page 163
To Redefine KVM Session Keyboard Shortcuts [Expert]	Page 157

▼ **To Configure Local User 1 and User 2 Sessions**

Perform this procedure if you want to redefine the parameters that apply to KVM port sessions when a local user is directly logged into the KVM/net.

1. In Expert mode, go to Configuration>KVM>General>.
2. To configure parameters for the User 1 port, select the User 1 tab.



3. To configure parameters for the User 2 port, select the User 2 tab.



The User 1 and User 2 forms are identical except that User 1 modifies the User 1 port options, while User 2 modifies the User 2 port options.

4. To change the idle timeout, enter a different number of minutes in the “Idle Timeout” field.
5. To change the screen saver timeout, enter a different number of minutes in the “Screen Saver Timeout” field.

6. To change the keyboard type, select a different keyboard from the “Keyboard type” pull-down menu.
7. To change the cycle time, enter a different number of seconds in the “Cycle Time” field.
8. To change any of the command key portions of KVM hot key combinations, enter a different letter in the “Quit,” “Power Management,” “Mouse/Keyboard Reset,” “Video Control,” “Switch Next,” “Switch Previous,” or “Port Info” fields.
9. Click “apply changes.”

▼ To Configure IP User (KVM Over IP) Sessions [Expert]

Perform this procedure if you want to redefine the parameters that apply to KVM port sessions when a remote user is connected through the Web Manager (in a KVM over IP session).

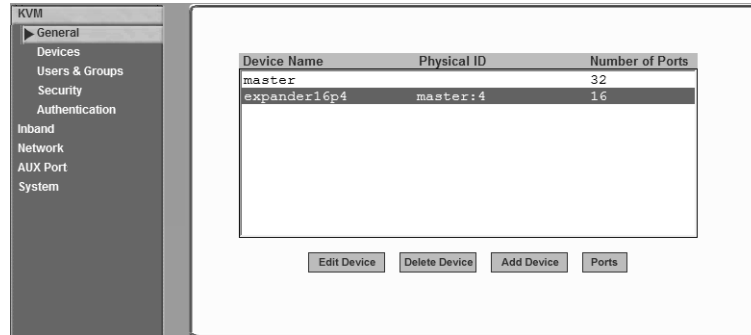
1. Go to Configuration>KVM>General> IP Users in Expert mode.

General	User 1	User 2	IP Users
Idle Timeout (min) <input type="text" value="3"/>			
TCP Viewer Ports <input type="text" value="5900+"/>			
Escape Sequences			
Quit	<input type="text" value="Q"/>	Power Management	<input type="text" value="P"/>
Mouse/Keyboard Reset	<input type="text" value="S"/>	Video Control	<input type="text" value="V"/>
Switch Next	<input type="text" value="N"/>	Switch Previous	<input type="text" value="P"/>
Port Info	<input type="text" value="I"/>		

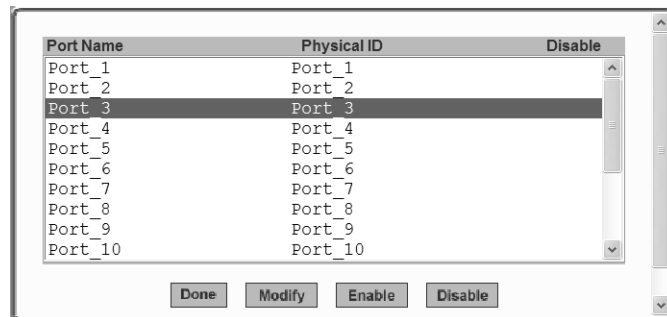
2. To change the idle timeout, enter a different number of minutes in the “Idle Timeout” field.
3. To change the TCP port number used by the AlterPath Viewer, enter another number in the “TCP Viewer Ports” field.
4. To change any of the command key portions of KVM hot key combinations, enter a different letter in the “Quit,” “Power Management,” “Mouse/Keyboard Reset,” “Video Control,” “Switch Next,” “Switch Previous,” or “Port Info” fields.
5. Click “apply changes.”

Modifying Individual KVM Ports

Selecting Configuration>KVM>Devices in Expert mode brings up the form shown in the following figure.

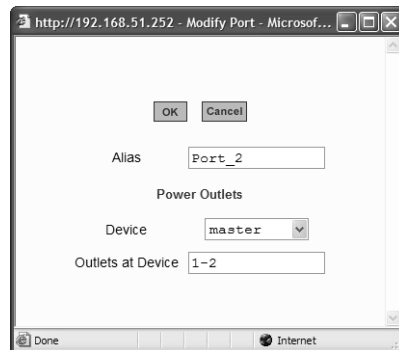


The device name “master” stands for the KVM/net, which is the master KVM unit in a cascaded configuration. Other device names may appear below “master” depending on the number of KVM units cascaded to the master. Selecting the name of a KVM unit in the list and clicking the “Ports” button brings up a list of the KVM ports on the KVM device, as shown in the following figure.



When you select one or more ports, you can enable or disable the KVM port(s) using the “Enable” or “Disable” buttons on the form.

When you select a port and click the “Modify” button, the dialog box shown in the following figure appears.



On the Modify Port dialog box, you can do the following:

- Configure an alias for a single KVM port
- Configure power management for the server that is connected to the KVM port while the user is logged into the server

The following table lists the related procedures with links to where they are described.

To Configure a KVM Port for Power Management [Expert]	Page 165
To Specify or Change the Alias for a KVM Port	Page 174
To Enable or Disable a KVM Port	Page 174

▼ **To Configure a KVM Port for Power Management [Expert]**

Perform this procedure to enable a user who is connected to a server through a KVM port to perform power management for the server while connected. When this procedure is completed, the user can manage up to two power connections for any one server. Before you start make sure the following prerequisites are complete:

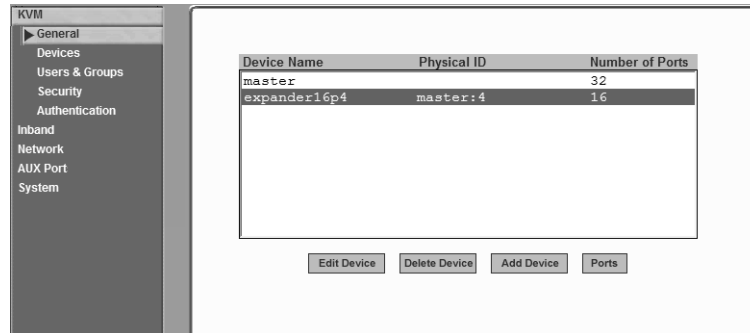
- The computer is plugged into an IPDU connected to the KVM/net's AUX port.
- The AUX port has been configured for power management.
See "To Configure an AUX Port for Power Management or PPP [Expert]" on page 252, if needed.
- You know the outlet number or numbers to which the computer's power cable or cables are plugged.

Configuring Cascaded KVM Units

The Devices form allows you to configure one or more secondary KVM units to a primary KVM unit, a process also known as cascading or daisy-chaining. See “Cascaded Devices” on page 24 for background information.

Selecting Configuration>KVM>Devices in Expert mode brings up the Devices form on which you can perform the following tasks:

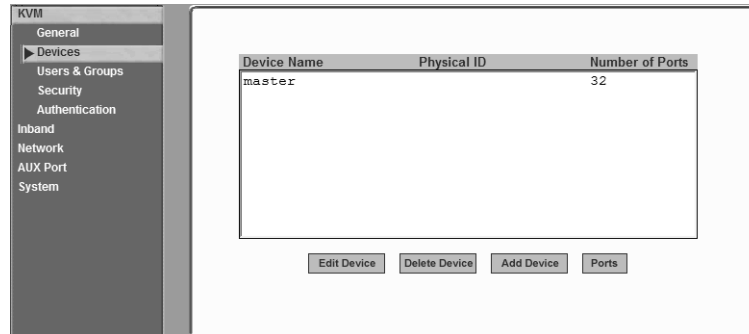
- Add a secondary KVM unit to be cascaded from the master KVM/net. See “To Add a Secondary KVM Unit to be Cascaded from the Master KVM/net” on page 167
- Edit the configuration of a cascaded device. See “To Edit the Configuration of a Cascaded KVM Unit” on page 168
- Delete the configuration of a cascaded device. See “To Delete the Configuration of a Cascaded KVM Unit” on page 170



▼ To Add a Secondary KVM Unit to be Cascaded from the Master KVM/net

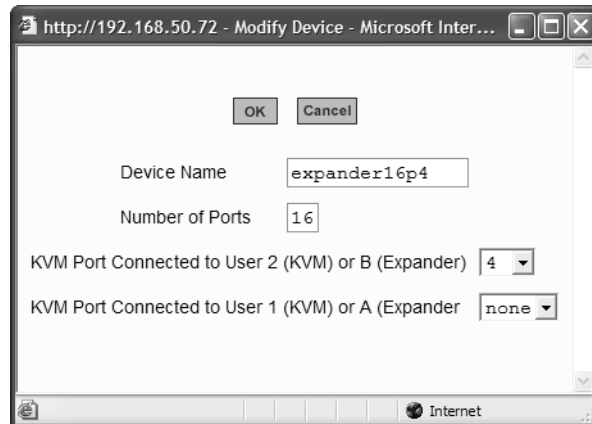
1. In Expert mode, go to: Configuration>KVM>Devices.

The Devices configuration form appears.



2. Click the Add Device button.

The Modify Device dialog box appears.



3. In the Device Name field, specify a name for the secondary device or KVM unit.
4. In the Number of Ports field, enter the number of ports contained in the cascaded device.

5. In the KVM Port Connected to User 2 (KVM) or B (Expander) drop-down list, enter the port number of the master KVM/net that is connected to the User 2 port of the secondary KVM device or the B port on the Expander.

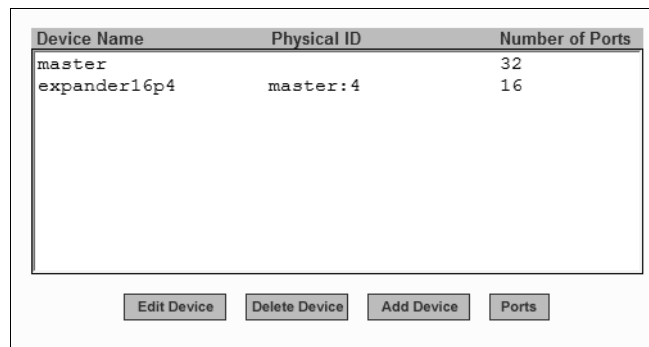
Note: See “Connecting Cascaded KVM Units to the Primary KVM/net” on page 115 for a background on the possible devices that can be cascaded and for instructions on connecting these devices to the master KVM/net.

6. In the Port Connected to User 1 or (KVM) or A (Expander) drop-down list, enter the secondary KVM port that is connected to the User 1 port of the primary KVM/net or the User A port on the Expander.
7. Click the OK button when done.
8. On the configuration window, select “apply changes” to save your configuration.

▼ **To Edit the Configuration of a Cascaded KVM Unit**

1. In Expert mode, go to: Configuration > KVM> Devices.

The Devices form appears.

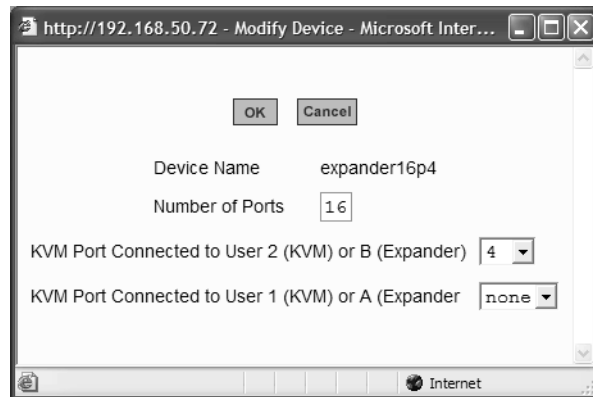


Device Name	Physical ID	Number of Ports
master		32
expander16p4	master:4	16

Buttons: Edit Device, Delete Device, Add Device, Ports

2. Select the item you wish to edit and click the Edit button.

The Modify Port dialog box appears.



3. In the Number of Ports field, enter the number of ports contained on the cascaded device.
4. To enable one user to access the ports on the cascaded kvm unit, in the KVM Port Connected to User 2 (KVM) or B (Expander) drop-down list, select the port number on the master KVM/net that is connected to the User 2 port on the secondary KVM device or the B port on the Expander.

Note: See “Connecting Cascaded KVM Units to the Primary KVM/net” on page 115 for a background on the possible devices that can be cascaded and for instructions on connecting these devices to the master KVM/net.

5. To enable two users to access the ports on the cascaded kvm unit, in the Port Connected to User 1 or (KVM) or A (Expander) drop-down list, enter the secondary KVM port that is connected to the User 1 port of the primary KVM/net or the User A port on the Expander.
6. Click the OK button.
7. Click “apply changes” to save your configuration.

▼ **To Delete the Configuration of a Cascaded KVM Unit**

1. In Expert mode, go to: Configuration > KVM> Devices.

The Devices form appears.

Device Name	Physical ID	Number of Ports
master		32
expander16p4	master:4	16

2. Select the item you wish to delete and click the Delete button.

The system deletes the selected device.

3. Click “apply changes” to save your configuration.

Modifying Individual KVM Ports

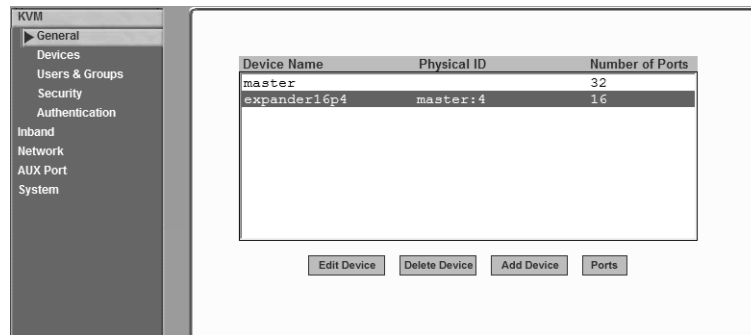
On the Modify Port dialog box, you can do the following:

- Configure an alias for a single KVM port
- Configure power management for the server that is connected to the KVM port while the user is logged into the server

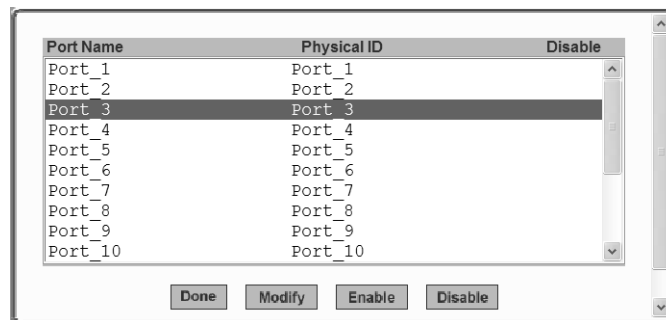
The following table lists the related procedures with links to where they are described.

To Configure a KVM Port for Power Management [Expert]	Page 165
To Specify or Change the Alias for a KVM Port	Page 174
To Enable or Disable a KVM Port	Page 174

Selecting Configuration>KVM>Devices in Expert mode brings up the form shown in the following figure.



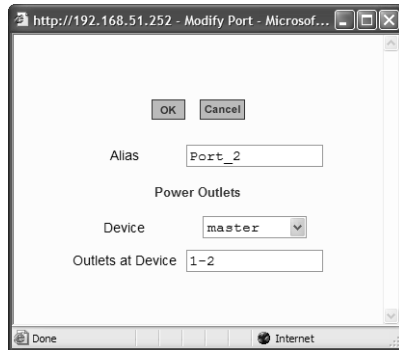
The device name “master” stands for the KVM/net, which is the master KVM unit in a cascaded configuration. Other device names may appear below “master” depending on the number of KVM units cascaded to the master. Selecting the name of a KVM unit in the list and clicking the “Ports” button brings up a list of the KVM ports on the KVM/net, as shown in the following figure.



When you select one or more ports, you can enable or disable the KVM port(s) using the “Enable” or “Disable” buttons on the form.

When you select a port and click the “Modify” button, the dialog box shown in the following figure appears.

Web Manager for Administrators



▼ **To Configure a KVM Port for Power Management [Expert]**

Perform this procedure to enable a user who is connected to a server through a KVM port to perform power management for the server while connected. When this procedure is completed, the user can manage up to two power connections for any one server. Before you start make sure the following prerequisites are complete:

- The computer is plugged into an IPDU connected to the KVM/net's AUX port.
 - The AUX port has been configured for power management.
See "To Configure an AUX Port for Power Management or PPP [Expert]" on page 252, if needed.
 - You know the outlet number or numbers to which the computer's power cable or cables are plugged.
1. In Expert mode, go to: Configuration > KVM> Devices.
The Devices form appears.
 2. Select the Device that contains the port(s) to be configured and click the Port button.
The Port Name list appears.

Port Name	Physical ID	Disable
FremWin98	Port_1	
FremNT	Port_2	
FremLin2	Port_3	
Port_4	Port_4	Yes
Port_5	Port_5	
Port_6	Port_6	Yes
Port_7	Port_7	
Port_8	Port_8	
Port_9	Port_9	
Port_10	Port_10	

Buttons: Done, Modify, Enable, Disable

3. Select the port you want to modify and click the Modify button.
The Modify Port dialog box appears.

4. In the Alias field, type an alias for the port
5. In the Device drop-down list, select the device that port is on.
The device could be the master KVM/net or a cascaded KVM unit.
6. In the Outlets at Device field, type the outlet number(s) of the IPDU that the server is plugged into.
Use commas (,) to separate outlets and use a hyphen (-) to indicate a range.
7. Click the OK button.
8. Click the “apply changes” button to save your configuration.

▼ **To Specify or Change the Alias for a KVM Port**

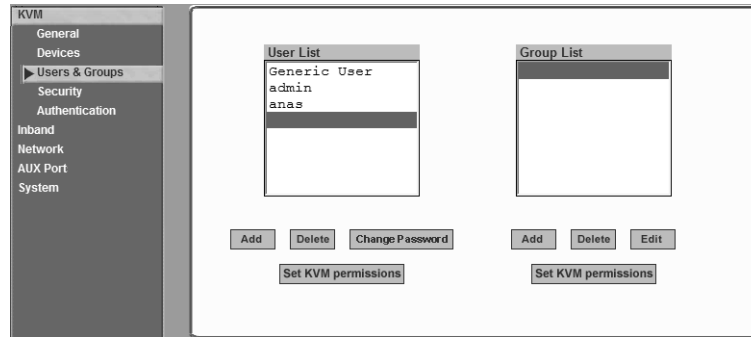
1. Go to Configuration>KVM >Devices in Expert mode, select the device that includes the port(s) you wish to modify.
2. Click the “Ports” button.
A list of all the selected ports appears.
3. Select a single port to be modified, and then select the “Modify” button.
The “Modify Port” dialog box appears.
4. To change the port’s alias, do the following steps.
 - a. Enter a new alias in the “Alias” field.
 - b. Click OK on the dialog box.
5. Click “Done” on the form listing all the ports.
6. Click “apply changes.”

▼ **To Enable or Disable a KVM Port**

1. Go to Configuration>KVM >Devices in Expert mode, and select the device that contains the port(s) you wish to enable or disable.
2. Click the “Ports” button.
A form listing all the selected ports appears.
3. Select the port(s) to be enabled or disabled, and then select the “Enable” or “Disable” button.
4. Click “Done” on the form listing all the ports.
5. Click “apply changes.”

Users & Groups

Selecting Configuration > KVM > Users & Groups in Expert mode brings up the form shown in the following figure.



You can use the Users & Groups form to do the following:

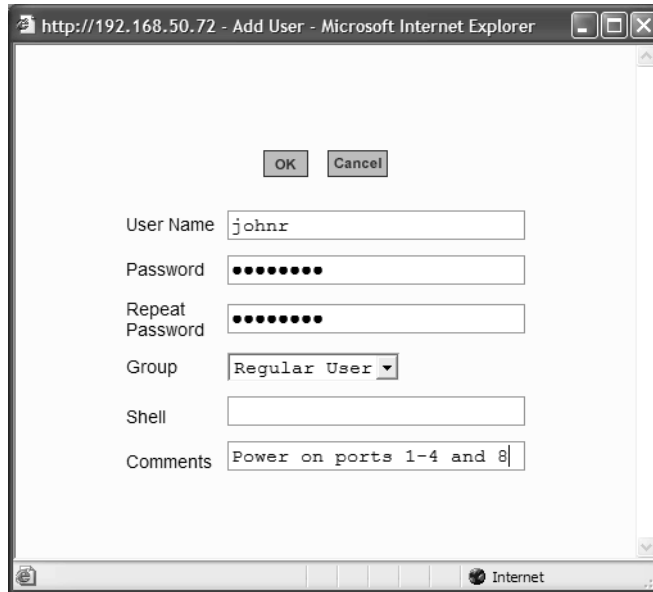
- Add or delete users.
- Assign or change user passwords.
- Reset the permissions of the Generic User.

Note: Permissions assigned to the Generic User define the default permissions for regular users.

- Set unique permissions for individual users.
- Assign permissions by group.
- Add or delete user groups from the Group Access List and assign users to a group.
- Restrict all users' access to devices connected to KVM ports by setting KVM permissions for users and groups of users for selected ports.

▼ **To Add a User [Expert]**

1. In Expert mode, go to Configuration>Users & Groups.
The Users & Groups form appears.
2. Click “Add.”
The “Add User” dialog box displays.



3. Either type the required information in the fields or select the desired option from the pull-down menu as shown in the previous screen and defined in the following table.

Field Name	Definition
User Name	Name of the user to be added.
Password	The password associated with the user name.
Group	On the left pull-down menu, select “Regular User [Default]” or “Admin.” Note: To configure a user to be able to perform all administrative functions, select the “Admin” group. See “Types of Users” on page 16 for more details.

Field Name	Definition
Shell	Optional. The default shell when the user makes an <code>ssh</code> or <code>telnet</code> connection with the switch. Choices are: <code>sh</code> or <code>bash</code> . The default is <code>sh</code> .
Comments	Optional notes about the user's role or configuration.

4. Click OK.
5. Click "apply changes."

▼ **To Delete a User or Group [Expert]**

1. In Expert mode, go to Configuration>Users & Groups.
The Users & Groups form displays.
2. Select the name of a user or group to delete.
3. Click "Delete."
4. Click "apply changes."

▼ **To Change a User's Password [Expert]**

1. In Expert mode, go to Configuration>Users & Groups.
The Users & Groups form displays.
2. Select the name of the user whose password you want to change.
3. Click "Change Password."
The Change User Password" dialog box displays.
4. Enter the new password in the "New Password" field and enter it again in the "Repeat New Password" field.
5. Click OK.
6. Click "apply changes."

▼ **To Add a Group [Expert]**

1. In Expert mode, go to Configuration>Users & Groups.
The Users & Groups form displays.
2. Under the list of groups, click “Add.”
The “Add Group” dialog box displays.
3. Type the name for the new group.
4. Type the usernames of the users you want to add to the group.
Use commas to separate the names.
5. Click OK.
6. Click “apply changes.”

▼ **To Modify a Group [Expert]**

1. In Expert mode, go to Configuration>Users & Groups.
The Users & Groups form displays.
2. Select the name of a group to modify.
3. Click “Edit.”
The “Edit Group” form displays.
4. Add or delete users from the group as desired.
5. Click OK.
6. Click “apply changes.”

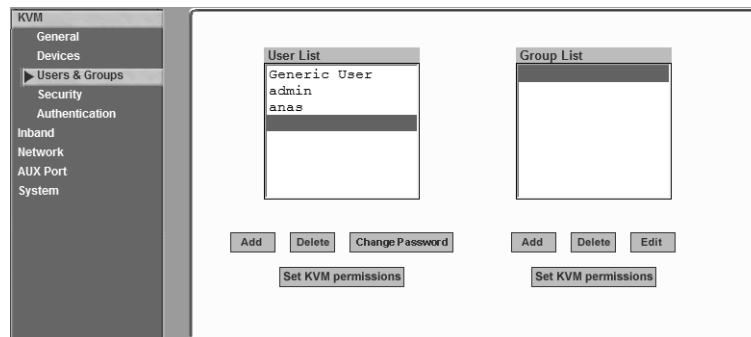
▼ To Select Users and Groups for Assigning KVM Port Access [Expert]

Perform this procedure to select users to access computers connected to KVM ports.

1. Go to Expert>Configuration > Users & Groups.

The Users & Groups form appears.

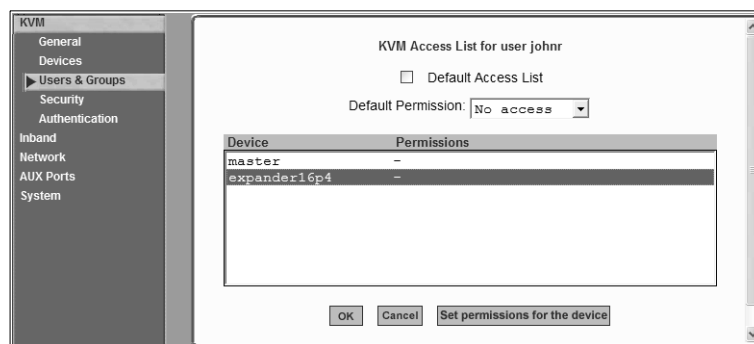
2. To set KVM port access for a regular user, select the name of the user or of multiple users from User List.



3. To set KVM port access permissions for a group, select the name of the group from the Group List.

4. Click the “Set KVM Permissions” button.

The “KVM Access list for “*username*” or “*groupname*” dialog box appears.



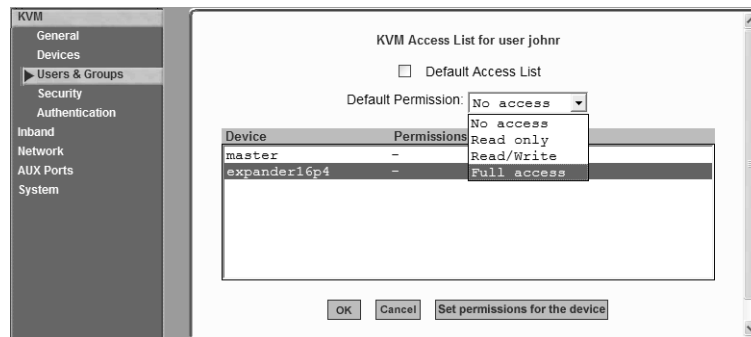
Note: When the “Default Access List” check box is checked, the user or group has the same permissions that are assigned to the Generic User. Changes made on this form when a username is selected convert the user into a non-generic user.

5. Go to “To Assign KVM Port Access to a User or Group” on page 180.

▼ **To Assign KVM Port Access to a User or Group**

Perform this procedure when you want to specify the types of access a user or group of users can have to computers that are connected to the KVM/net’s KVM ports.

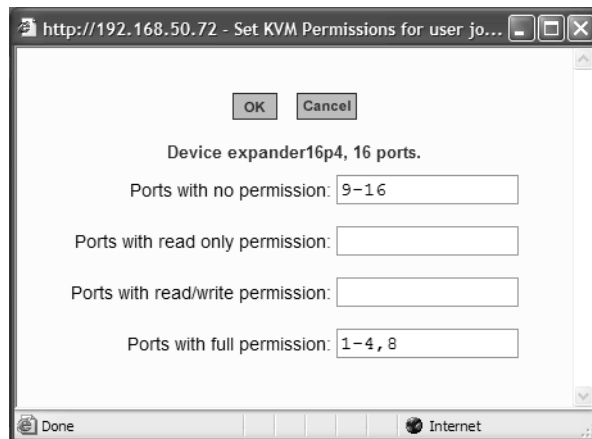
1. Go to Expert>Configuration >Users & Groups, and select a user or group.
If needed see “To Select Users and Groups for Assigning KVM Port Access [Expert]” on page 179.
2. To assign to the selected user or group the same permissions assigned to the Generic User, make sure the “Default Access List” check box is checked and click OK.
3. To re-define the KVM permissions for the selected user or group, clear the check box.
4. Select the desired access option from the “Default Permission:” pull-down menu.



As shown in the previous screen example, the options are: “No access,” “Read only,” “Read/Write,” “Full access.”

5. To configure access to a device and all of its ports, do the following:
 - a. Select one or more devices from the Device list.
 - b. From the Default Permissions drop-down list, select the permissions you wish to apply.
 - c. Go to Step 8.
6. To configure access to individual ports or groups of ports, do the following:
 - a. Select a device from the Device list.
 - b. Click the “Set permissions for the device” button.

The “Set KVM Permissions for the device” dialog box displays as shown in the following screen example. (The example shows the dialog box when the “master” device is selected.)



In the fields for each desired category, type either port aliases or numbers, separating them either by commas or dashes.

7. Click OK.

The newly-set permissions appear next to the Device name in the Permissions column, as shown in the following screen example, which shows the restrictions applied to the user name “ana.”

Web Manager for Administrators

KVM Access List for user johnr

Default Access List

Default Permission: No access

Device	Permissions
master	-
expander16p4	9-16:none/1-4,8:full

OK Cancel Set permissions for the device

The following screen example illustrates how the previous settings affect access to ports. When an individual or member of a group with the access permissions shown in the previous screen logs into the Web Manager, the list of ports displayed does not include ports 9 to 16 (because they were configured with no access).

Connect to server

IPDU Power Mgmt.

Port 1 (KVM)

- Port 1 (KVM)
- PC243 (KVM)
- Port_3 (KVM)
- Port_4 (KVM)
- Port_5 (KVM)
- Port_6 (KVM)
- Port_7 (KVM)
- Port_8 (KVM)

8. Click OK.
9. Click “apply changes.”

Security

Selecting Configuration>KVM>Security in Expert mode brings up the form shown in the following figure. Administrators can specify that communications are encrypted between the KVM/net and any computer attached to a KVM port.

The Security form allows you to configure your IP security with the following levels:

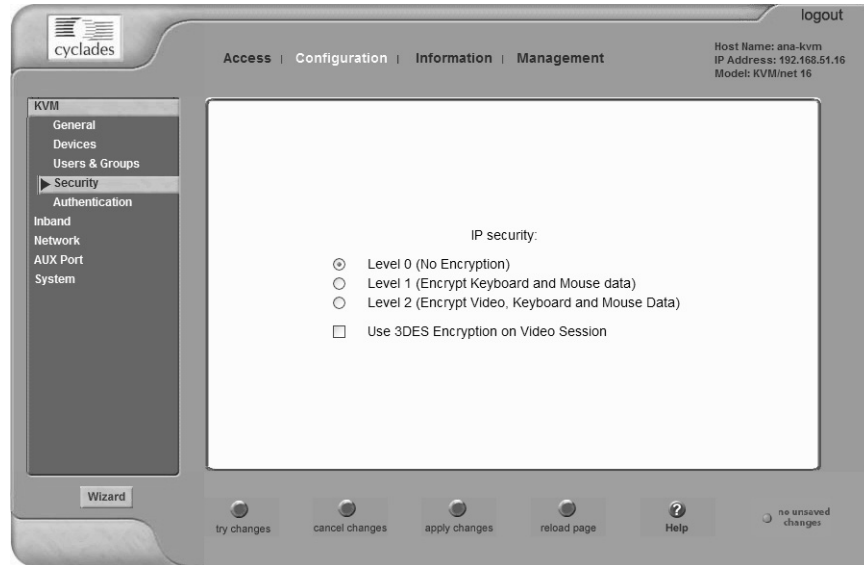
- Level 0 (No Encryption)
- Level 1 (Encrypt Keyboard and Mouse data)
- Level 2 (Encrypt Video, Keyboard and Mouse Data)

In addition, you can select 3DES (Triple Data Encryption Standard) for video sessions in stead of RC4 (Rivest Cipher four), the system default. Though RC4 is faster than 3DES, it is less secure.

▼ **To Configure Encryption on Port Connections [Expert]**

1. In Expert mode, go to: Configuration > KVM > Security.

The Security form appears.



The screenshot shows the 'Security' configuration page in the Web Manager for Administrators. The page is titled 'cyclades' and has a navigation bar with 'Access | Configuration | Information | Management'. The 'KVM' section is expanded, showing 'General', 'Devices', 'Users & Groups', 'Security', 'Authentication', 'Inband', 'Network', 'AUX Port', and 'System'. The 'Security' page displays the 'IP security' configuration options:

- Level 0 (No Encryption)
- Level 1 (Encrypt Keyboard and Mouse data)
- Level 2 (Encrypt Video, Keyboard and Mouse Data)
- Use 3DES Encryption on Video Session

At the bottom of the page, there are buttons for 'try changes', 'cancel changes', 'apply changes', 'reload page', 'Help', and 'no unsaved changes'.

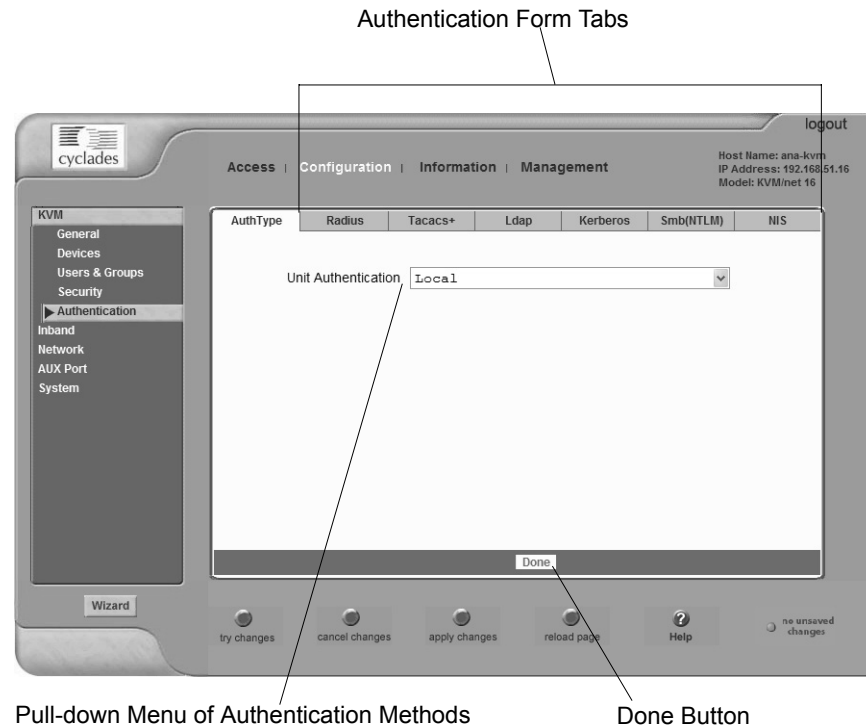
2. Check the appropriate radio buttons.

RC4 is the default encryption if 3DES is not selected. See “Security” on page 183, if needed, for more information.

3. Click “apply changes” to complete the procedure.

Configuring an Authentication Method

Configuration > KVM > Authentication in Expert mode brings up the form shown in the following figure.



The administrator uses the Authentication forms for two main purposes:

- To select an authentication method for the KVM/net *only*.
The default authentication method for the KVM/net is Local. The administrator can either accept the default or select one of the other authentication methods from the pull-down menu on the AuthType form. See “To Configure an Authentication Method for KVM/net Logins” on page 186 for the procedure.
Any authentication method chosen for the KVM/net is used for authentication of any users attempting access through telnet, ssh, or the Web Manager.

See “Authentication” on page 44 for more details.

- To configure all authentication servers for the KVM/net ports.

The administrator fills out one of the tabbed forms to set up an authentication server for each authentication method to be used by the KVM/net and by any of its ports: RADIUS, TACACS+, LDAP, Kerberos, SMB (ports only), NIS. See “Configuring Authentication Servers for Logins to the KVM/net and Connected Devices” on page 188.

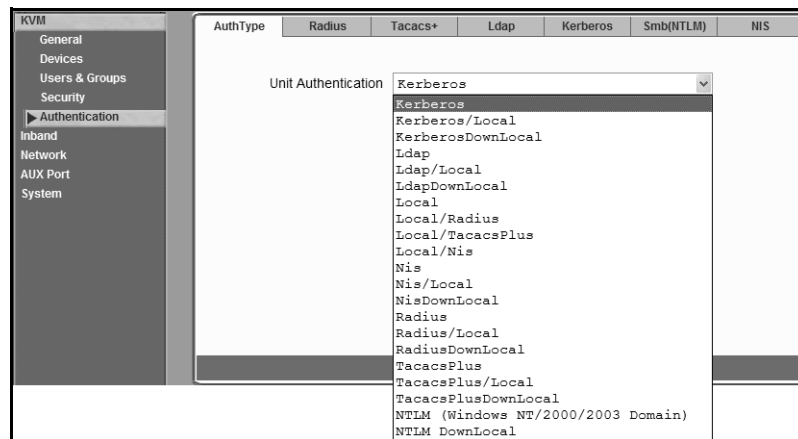
See “To Configure an Authentication Method for Logins Through KVM Ports” on page 187 for instruction on how to specify an authentication method for ports.

▼ To Configure an Authentication Method for KVM/net Logins

See “Configuring an Authentication Method” on page 185, if needed, for background information.

1. Go to Configuration>KVM>Authentication in Expert mode.

The AuthType form displays, as shown in the following figure.



2. To specify an authentication method for logins to the KVM/net, select a method from the Authentication pull-down menu.
3. Make sure that an authentication server is specified for the selected authentication type.

See “Configuring Authentication Servers for Logins to the KVM/net and Connected Devices” on page 188.

▼ **To Configure an Authentication Method for Logins Through KVM Ports**

By default, all users can log into all ports. This procedure configures a single authentication method that applies whenever anyone attempts to log into a device connected to any KVM port.

1. Go to Expert>Configuration>General.

The General form displays.

2. Select an Authentication Type from the pull-down menu.

The default option is None.

3. Make sure that an authentication server is specified for the selected authentication type.

See “Configuring Authentication Servers for Logins to the KVM/net and Connected Devices” on page 188.

Configuring Authentication Servers for Logins to the KVM/net and Connected Devices

The administrator fills out the appropriate form to set up an authentication server for every authentication method to be used by the KVM/net and by any of its ports: Kerberos, LDAP, NIS, NTLM/SMB (ports only), RADIUS, TACACS+.

The following table lists the procedures that apply to each authentication method.

Method	Variations	Procedures
Kerberos	Kerberos, Local/Kerberos, Kerberos/Local, or Kerberos/DownLocal	“To Identify a Kerberos Authentication Server [Expert]” on page 161
LDAP	LDAP, Local/LDAP, LDAP/Local, or LDAP/DownLocal	“To Identify an LDAP Authentication Server [Expert]” on page 163
NIS	NIS, Local/NIS, NIS/Local, or NIS/DownLocal	“To Configure a NIS Authentication Server [Expert]” on page 165
NTLM (Windows NT/2000/2003 Domain)	NTLM (Windows NT/2000/2003 Domain), or NTLM/DownLocal	“To Configure an SMB(NTLM) Authentication Server [Expert]” on page 165
RADIUS	RADIUS, Local/RADIUS, RADIUS/Local, or RADIUS/DownLocal	“To Identify a RADIUS Authentication Server [Expert]” on page 166
TACACS+	TACACS+, Local/TACACS+, TACACS+/Local, or TACACS+/DownLocal	“To Identify a TACACS+ Authentication Server [Expert]” on page 167

▼ **To Identify a Kerberos Authentication Server**

Perform this procedure to identify the authentication server when the KVM/net or any of its ports is configured to use the Kerberos authentication method or any of its variations (Kerberos, Local/Kerberos, Kerberos/Local, or KerberosDownLocal.)

Before starting this procedure, find out the following information from the Kerberos server's administrator:

- Realm name and KDC address
- Host name and IP address for the Kerberos server

Also, work with the Kerberos server's administrator to ensure that following types of accounts are set up on the Kerberos server and that the administrators of the KVM/net and connected devices know the passwords assigned to the accounts:

- An account for "admin"
 - If Kerberos authentication is specified for the KVM/net, accounts for all users who need to log into the KVM/net to administer connected devices.
 - If Kerberos authentication is specified for KVM ports, accounts for users who need administrative access to connected devices
1. Make sure an entry for the KVM/net and the Kerberos server exist in the KVM/net's `/etc/hosts` file.
 - a. Go to Configuration>Network>Host Table in Expert mode.
The "Host Table" form appears.
 - b. Add an entry for KVM/net if none exists and an entry for the Kerberos server.
 - i. Click "Add."
The "New/Modify Host" dialog appears.
 - ii. Enter the address in the "IP Address" field.
 - iii. Enter the name in the "Name" field.
 - iv. If desired, enter an optional alias in the "Alias" field.
 2. Make sure that timezone and time and date settings are synchronized on the KVM/net and on the Kerberos server.

Web Manager for Administrators

Time and date synchronization is most easily achieved by setting both to use the same NTP server.

- a. To specify an NTP server, follow the procedure under “To Configure Time and Date Using an NTP Server” on page 256.
 - b. To manually set the time and date on the KVM/net, follow “To Manually Set the Time and Date” on page 255.
 - c. Work with the authentication server’s administrator to synchronize the time and date between the KVM/net and the server.
- 3.** If the KVM/net is not located in the PST time zone, set the timezone on the KVM/net.
- a. Make a console connection to the KVM/net and log in as root,

```
KVM login: root
Password: *****
```

The root prompt appears.

```
[root@kvm root]#
```

- b. Enter **set_timezone**.

A list of timezones appears followed by a prompt asking you to enter a number of a timezone.

```
[root@kvm root]# set_timezone
Please choose the time zone where this machine is located.
0) GMT
1) 1h West GMT
2) 10h West GMT
...
26) 9h East GMT
Enter your option:
```

- c. Enter the number of the timezone where the KVM/net is located.

```
Enter your option: 10
```

- d. Logout from the console session and close the terminal.

4. In the Web Manager Expert mode, go to Configuration>Authentication>Kerberos.

The Kerberos form displays as shown in the following figure.

The screenshot shows a configuration window with several tabs: AuthType, Radius, Tacacs+, Ldap, Kerberos, Smb(NTLM), and NIS. The 'Kerberos' tab is selected. Below the tabs, there are two text input fields. The first is labeled 'Kerberos Server (Realm)' and is currently empty. The second is labeled 'Kerberos Realm Domain Name' and contains the text 'cyclades.com'. At the bottom of the window, there is a 'Done' button.

5. Fill in the form according to your local setup of the Kerberos server.
6. Click “Done.”
7. Click “apply changes.”

▼ **To Identify an LDAP Authentication Server [Expert]**

Perform this procedure to identify the authentication server when the KVM/net or any of its ports is configured to use the LDAP authentication method or any of its variations (LDAP, Local/LDAP, LDAP/Local, or LDAP/DownLocal).

Before starting this procedure, find out the following information from the LDAP server’s administrator:

- The distinguished name of the search base
- The LDAP domain name
- Whether to use secure LDAP
- The authentication server’s IP address

You can enter information in the following two fields, but an entry is not required:

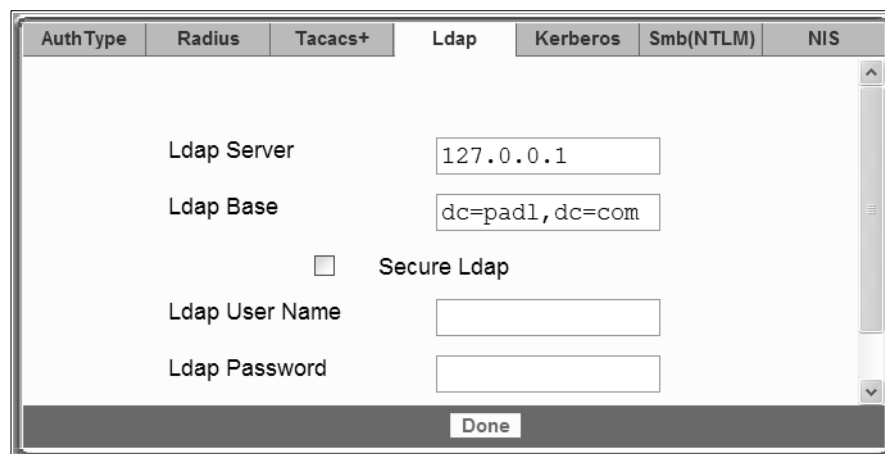
- The LDAP password
- The LDAP user name

Web Manager for Administrators

Work with the LDAP server's administrator to ensure that following types of accounts are set up on the LDAP server and that the administrators of the KVM/net and connected devices know the passwords assigned to the accounts:

- An account for “admin”
 - If LDAP authentication is specified for the KVM/net, accounts for all users who need to log into the KVM/net to administer connected devices.
 - If LDAP authentication is specified for KVM ports, accounts for users who need administrative access to the connected devices.
1. Go to Configuration>Authentication>LDAP in Expert mode.

The “LDAP” form displays with “LDAP Server” and “LDAP Search Base” fields filled in from the current values in the `/etc/ldap.conf` file.



The screenshot shows a web-based configuration interface for LDAP authentication. At the top, there are several tabs: 'AuthType', 'Radius', 'Tacacs+', 'Ldap', 'Kerberos', 'Smb(NTLM)', and 'NIS'. The 'Ldap' tab is currently selected. Below the tabs, there are several input fields and a checkbox. The 'Ldap Server' field contains the IP address '127.0.0.1'. The 'Ldap Base' field contains the distinguished name 'dc=padl,dc=com'. There is a checkbox labeled 'Secure Ldap' which is currently unchecked. Below this, there are two more input fields: 'Ldap User Name' and 'Ldap Password', both of which are currently empty. At the bottom right of the form, there is a 'Done' button.

2. Supply the IP address of the LDAP server in the “LDAP Server” field.
3. If the LDAP authentication server uses a different distinguished name for the search base than the one displayed in the “LDAP” Base field, change the base definition.

The default distinguished name is “dc,” as in `dc=value,dc=value`. If the distinguished name on the LDAP server is “o,” then replace `dc` in the base field with `o`, as in `o=value,o=value`.

4. Replace the default base name with the name of your LDAP domain.
For example, for the LDAP domain name cyclades.com, the correct entry is: `dc=cyclades,dc=com`.

5. Click “Done.”

6. Click “apply changes.”

The changes are stored in `/etc/ldap.conf` on the KVM/net.

▼ **To Configure an SMB(NTLM) Authentication Server [Expert]**

Perform the following to identify the authentication server if any of the ports is configured to use the NTLM (Windows NT/2000/2003 Domain) authentication method or NTLM/Downlocal.

1. Go to Configuration>Authentication>SMB(NTLM) in Expert mode.

The SMB(NTLM) form displays as shown in the following figure.

The screenshot shows a configuration window with a tabbed interface. The tabs are: AuthType, Radius, Tacacs+, Ldap, Kerberos, Smb(NTLM), and NIS. The Smb(NTLM) tab is active. The form contains the following fields:

- Domain:
- Primary Domain Controller:
- Secondary Domain Controller:

A "Done" button is located at the bottom right of the form.

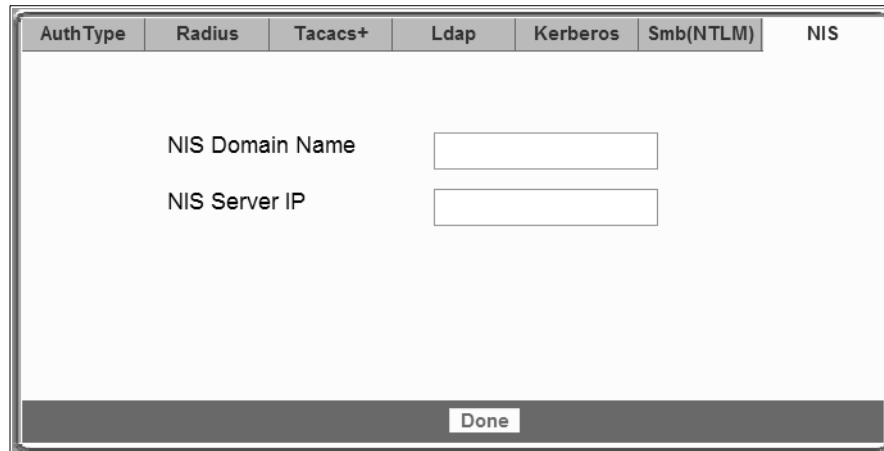
2. Fill in the form according to your configuration of the SMB server.
3. Click “Done.”
4. Click “apply changes.”

▼ **To Configure a NIS Authentication Server [Expert]**

Perform this procedure to identify the authentication server when the KVM/net or any of its ports is configured to use the NIS authentication method or any of its variations (Local/NIS, NIS/Local, or NIS/DownLocal).

1. Go to Configuration>Authentication>NIS in Expert mode.

The NIS form displays as shown in the following figure.



The screenshot shows a web-based configuration interface for NIS authentication. At the top, there is a horizontal row of tabs: 'AuthType', 'Radius', 'Tacacs+', 'Ldap', 'Kerberos', 'Smb(NTLM)', and 'NIS'. The 'NIS' tab is currently selected. Below the tabs, the form contains two text input fields. The first field is labeled 'NIS Domain Name' and the second is labeled 'NIS Server IP'. At the bottom of the form, there is a 'Done' button.

2. Fill in the form according to your configuration of the NIS server.
3. Click “Done.”
4. Click “apply changes.”

▼ **To Identify a RADIUS Authentication Server [Expert]**

Perform this procedure to identify the authentication server when the KVM/net or any of its ports is configured to use the RADIUS authentication method or any of its variations (Local/RADIUS, RADIUS/Local, or RADIUS/DownLocal).

1. Go to Configuration>Authentication>RADIUS in Expert mode.

The RADIUS form displays as shown in the following figure.

AuthType	Radius	Tacacs+	Ldap	Kerberos	Smb(NTLM)	NIS
	First Authentication Server					
	Second Authentication Server					
	First Accounting Server					
	Second Accounting Server					
Done						

2. Fill in the form according to your local setup of the RADIUS server or servers.
3. Click “Done.”
4. Click “apply changes.”

The changes are stored in `/etc/raddb/server` on the KVM/net.

▼ **To Identify a TACACS+ Authentication Server [Expert]**

Perform this procedure to identify the authentication server when the KVM/net or any of its ports is configured to use the TACACS+ authentication method or any of its variations (Local/TACACS+, TACACS+/Local, or TACACS+/DownLocal).

1. Go to Configuration>Authentication>TACACS+ in Expert mode.

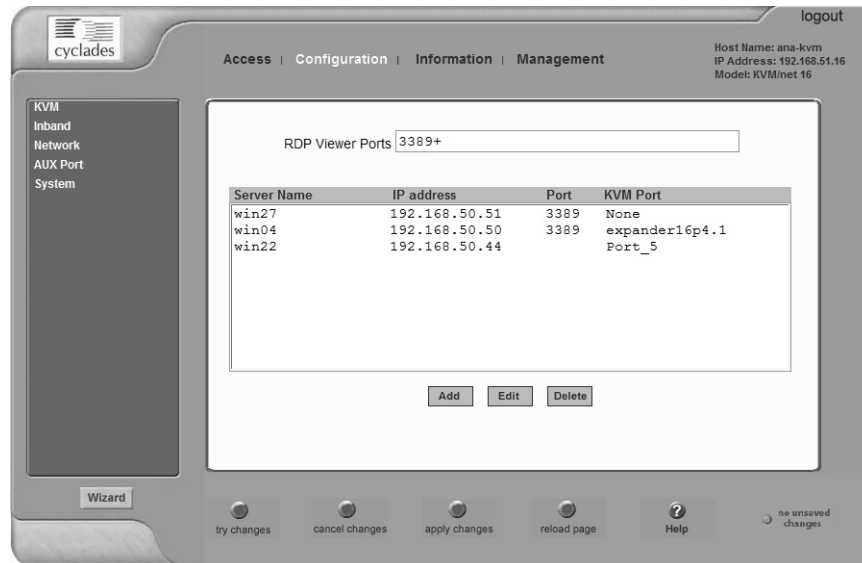
The TACACS+ form appears.

AuthType	Radius	Tacacs+	Ldap	Kerberos	Smb(NTLM)	NIS
		First Authentication Server	192.168.49.125			
		Second Authentication Server				
		First Accounting Server	192.168.49.125			
		Second Accounting Server				
Done						

2. Fill in the form according to your local setup of the TACACS+ server or servers.
3. Click “Done.”
4. Click “apply changes.”
5. The changes are stored in `/etc/tacplus.conf` on the KVM/net.

Configuring In-band (RDP) Servers

Selecting Configuration>Inband in Expert mode brings up the form displayed in the following figure.



You can use the Add, Modify, and Delete buttons to configure in-band server connections to Windows Terminal Servers using RDP. Up to either 16 or 32 in-band servers can be configured on a KVM/net depending on the model ordered.

If secondary KVM/net units are cascaded to the master KVM/net, administrators can configure additional in-band servers. The total number of in-band servers configured is the same as the total number of KVM ports in the whole infrastructure (master and cascaded devices). Even though it is possible to configure a KVM port on the master or on any cascaded device for each in-band server, all in-band configuration and connections are done through the master KVM/net.

For more complete access and as a backup to in-band connection failures, in-band servers can also be connected to KVM ports on the KVM/net. This enables out-of-band access to the in-band server so that if the in-band connection fails, the user is able to reconnect to the server using a KVM connection. This also enables users to view the BIOS, POST, and boot messages for server administration.

See “Server Access: In-band and Out of Band” on page 36, for a description of the differences between in-band and KVM connections.

Prerequisites for In-band Access to RDP Servers

The following prerequisites must be met in order for a KVM/net in-band connection to work:

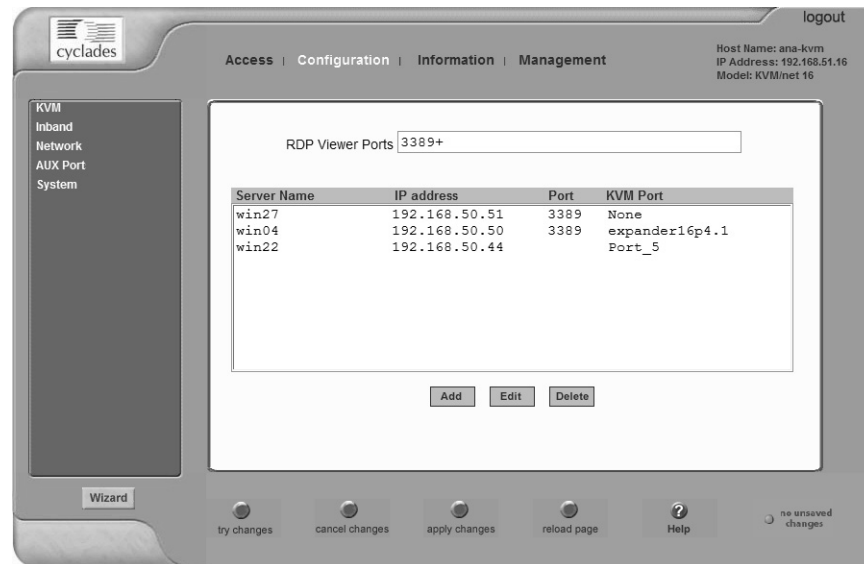
- The connected server must be a Windows (Win2000, 2003, XP, and NT) Terminal Server with RDP enabled.
Windows Terminal Servers do not have RDP enabled by default: The administrator of these servers must enable RDP on the server in order for the KVM/net in-band connection to work.
- A KVM/net user who needs to access any in-band server must have the following:
 - A valid account created on the in-band server.
The KVM/net does not authenticate or offer permissions configuration for in-band connections.
 - Internet access and Microsoft Internet Explorer 6 on a remote Windows client machine.
- The Windows Terminal Server must be configured on the in-band page of the Web Manager. See “To Add or Modify an In-band (RDP) Server” on page 199 for configuration instructions.
- If you want to enable an out-of-band, KVM connection as back up for an in-band connection failure or if you want to view the BIOS, POST, and boot messages on the server, the RDP server must be connected to a KVM port on the master KVM/net or on a cascaded and configured KVM unit.
See “To Connect Computers to KVM Ports” on page 72 for instructions on physically connecting a server to a KVM/net port.

▼ To Add or Modify an In-band (RDP) Server

See the previous section “Prerequisites for In-band Access to RDP Servers” on page 198 for prerequisite information to this procedure.

1. In Expert mode, go to: Configuration>Inband.

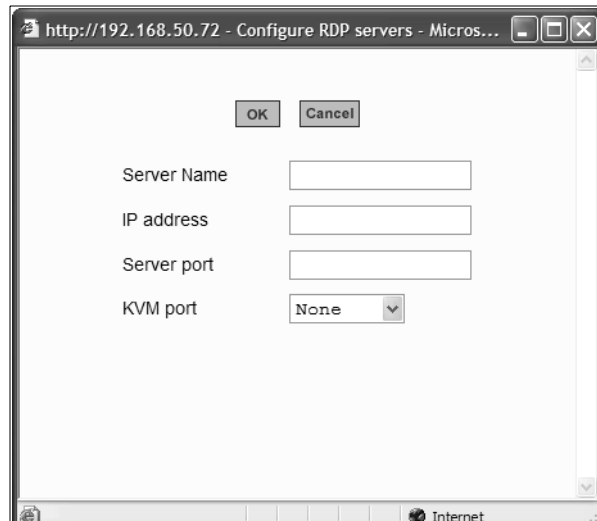
The Inband form appears.



2. To add a server to the list, click Add.

The Configure RDP Servers dialog box appears.

Web Manager for Administrators

A screenshot of a web browser window titled "http://192.168.50.72 - Configure RDP servers - Micros...". The window contains a form with the following fields: "Server Name" (text input), "IP address" (text input), "Server port" (text input), and "KVM port" (dropdown menu with "None" selected). At the top of the form are "OK" and "Cancel" buttons. The browser's address bar and status bar are visible at the bottom.

The connected server must be a Windows (Win2000 or NT) Terminal Server with RDP enabled.

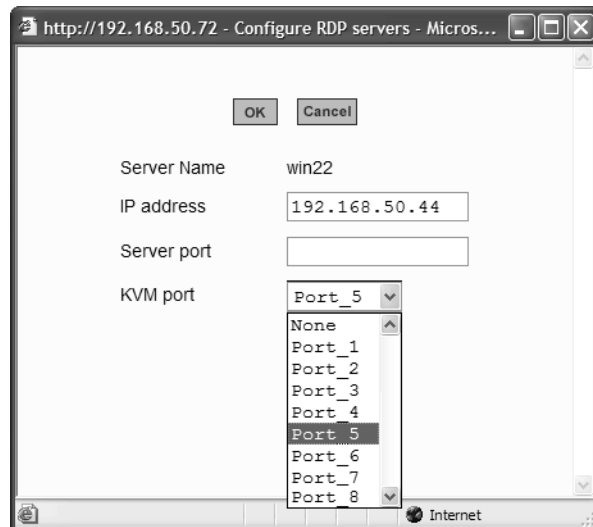
3. To modify a server, select the server on the list and click Modify.
4. In the Server Name field, specify a unique name for the in-band server.
This name will appear in the drop-down list on the Connect to Server form.

Note: Once a name is given to an in-band server, it cannot be modified. In order to change the name of an in-band server, you must delete the server configuration and add the server again to the KVM/net.

5. In the IP Address field, enter the IP address of the in-band server.
6. (Optional) In the Server Port field, specify a port to be used if it differs from the default which is 3389.

All servers with RDP enabled are configured with 3389 as the default port unless the administrator of the RDP server changes it.

7. To enable a back up KVM connection for the in-band server, from the KVM Port drop-down list, select the KVM port to which the in-band server is connected.



This enables both in-band and out-of-band access to the connected server. If the in-band connection fails or if an RDP session already exists, the user is able to reconnect to the server using a KVM connection. This also enables users to view the BIOS, POST, and boot messages for server administration.

8. Click OK to close the dialog box.
9. Specify the TCP ports or a range of TCP ports to be used in the RDP Viewer Ports field.

You must have at least eight valid TCP ports specified in order to have up to eight simultaneous in-band connections through the KVM/net.

For example, if you want ports 3389 to ports 10000 to be used, type “3389 - 10000”. If you want to use ports 3389 and higher, type “3389+”. If you want to use ports 3389 and below, type “3389-”.

You can request valid TCP ports from your network administrator.

10. Click “apply changes.”
11. Repeat steps 1-9 for every in-band server connection required.

The KVM/net supports the configuration of up to 16 or 32 in-band servers depending on the number of KVM ports on the KVM/net model ordered.

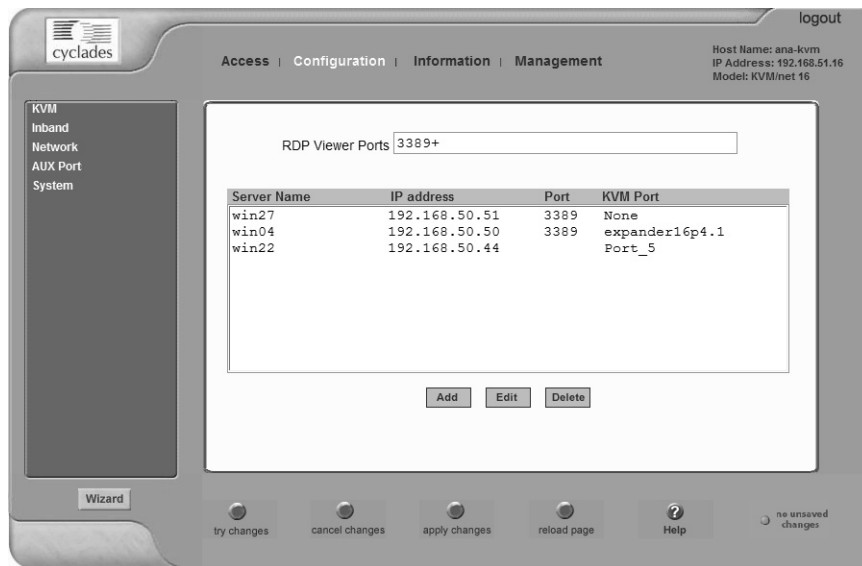
12. To connect to the in-band server, in Expert mode, go to Access>Connect to Server.

See “To Connect to Servers Through The Web Manager’s Connect To Server Form” on page 290.

▼ **To Delete an In-band (RDP) Server**

1. In Expert mode, go to: Configuration>Inband.

The Inband form appears.



2. Select the in-band server from the list and click Delete.
3. Click “apply changes.”

Network

Selecting Configuration > Network in Expert mode brings up the following form.

Network configuration comprises eight forms:

Table 4-1: Network Forms

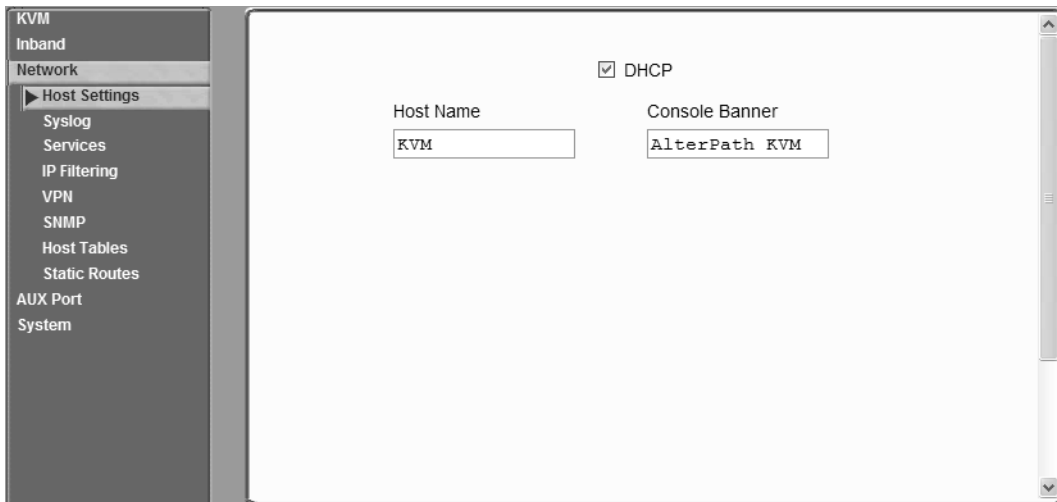
Form	Use this form to:
Host Settings	Configure host connections, including: Ethernet Port connections, DNS Service, and Name Service Access.
Syslog	Define the Syslog Servers to enable system logging.
PCMCIA Management	Configure one of the PCMCIA card slots for use with a modem card.
Services	Define or activate the method of access (<i>i.e.</i> , Telnet, SSH, SNMP, Client, or NTP).

Table 4-1: Network Forms (Continued)

Form	Use this form to:
IP Filtering	Configure the selective filtering of packets that may potentially crack your network system or generate unnecessary traffic.
VPN	Configure IPsec tunnels to establish a secure connection between KVM/net and a security gateway machine.
SNMP	Configure the SNMP server to manage complex networks.
Host Table	View hosts list; add, edit, and delete hosts.
Static Routes	View, create, and delete routes from the table.

Host Settings

When Configuration>Network>Syslog is selected in Expert mode, the form shown in the following figure appears.



If the “DHCP” check box is not checked, then other options appear on the form as shown in the following example.

The screenshot shows the 'Host Settings' configuration page in the KVM management interface. On the left is a navigation menu with options like 'KVM', 'Inband', 'Network', 'Host Settings', 'Syslog', 'Services', 'IP Filtering', 'VPN', 'SNMP', 'Host Tables', 'Static Routes', 'AUX Port', and 'System'. The main area contains the following configuration fields:

- DHCP
- Host Name: ana-kvm
- Console Banner: AlterPath KVM
- Ethernet Port: (empty)
- Primary IP: 192.168.51.16
- Network Mask: 255.255.252.0
- Secondary IP: (empty)
- Secondary Network Mask: (empty)
- MTU: 1500
- DNS Service: (empty)
- Primary DNS Server: 192.168.44.21
- Secondary DNS Server: (empty)

▼ To Configure Host Settings [Expert]

The Host Settings form allows you to configure the network settings for the KVM/net.

1. Go to Expert>Network>Host Settings.

The Host Settings form appears.

2. By default, the DHCP is enabled. To disable DHCP, clear the DHCP check box.

The system adds the Ethernet Port and DNS Service sections.

3. Complete or edit the fields described in the following table as necessary.

Table 4-2: Host Settings Configuration Fields

Field Name	Definition
Host Name	The fully qualified domain name identifying the specific host computer within the Internet.
Console Banner	A text string designed to appear on the console upon logging into and exiting from a port as a way to verify or identify the particular port connection.

Table 4-2: Host Settings Configuration Fields (Continued)

Field Name	Definition
Ethernet Port	
Primary IP	The 32-bit numeric IP address of the KVM/net unit on the Internet.
Network Mask	The 32-bit number used to group IP addresses together or to indicate the range of IP addresses for this IP network/subnet/supernet.
Secondary IP	The 32-bit numeric, secondary IP address of the KVM/net unit on the Internet.
Secondary Network Mask	The network mask of the secondary IP.
MTU	Maximum Transmission Unit used by the TCP protocol.
DNS Service	
Primary DNS Server	Address of the Domain Name Server.
Secondary DNS Server	Address of the backup Domain Name Server.
Domain Name	The name that identifies the domain (e.g., domainname.com).
Gateway IP	The gateway numeric identification number.

4. Select “apply changes” when done to save your configuration to flash.

Syslog

When Configuration>Network>Syslog is selected in Expert mode, the form shown in the following figure appears.

You can use the Syslog form to configure how the KVM/net handles syslog messages. The Syslog form allows you to do the following:

- Specify one or more syslog servers to receive syslog messages related to ports.
- Specify rules for filtering messages.

The top of the form is used to tell the KVM/net where to send syslog messages:

- You can specify one facility number for messages from KVM ports and AUX ports and another facility number for messages from KVM ports. Obtain the facility numbers to use from the syslog server's administrator. See "To Add a Syslog Server [Wizard]" on page 140 for how syslogging is configured for the KVM/net under the Configuration>General form. You can specify the same or different syslog servers and the same or duplicate facility numbers according to your site's configuration.
- You can send syslog messages to the console port (for logging the messages even if no user is logged in); to all sessions where the root user is logged in, or to one or more syslog servers.
- You can add or delete entries for syslog servers.

The bottom of the form has check boxes for specifying which types of messages are forwarded based on the following criteria:


- Their severity level: "Emergency," "Alert," "Critical," "Error," "Warning," "Notice," "Info," "Debug"
- Their category "CAS/AUX log," "KVM log," "Data Buffering log," "Web log," or "System log."

▼ **To Configure Syslogging for KVM Ports and Specify Message Filtering [Expert]**

1. Go to Configuration>Network>Syslog in Expert mode.
The Syslog form displays.
2. Select a destination for the Syslog messages by clicking the check box next to one or all of the options: "Console," "Root User," or "Server."
3. Add a syslog server to the Syslog Servers list, by entering its IP address in the "New Syslog Server" field, and clicking the "Add>>" button.
4. Select a facility number for messages generated by KVM or AUX ports by selecting the number from the "CAS/AUX Ports Facility" pull-down menu.
5. Select a facility number for messages generated by KVM ports by selecting the number from the "KVM Ports Facility" pull-down menu.
6. Click "apply changes."

Services

Selecting Configuration>Network>Services in Expert Mode, brings up the following form.



The screenshot shows a configuration interface for 'Services'. On the left is a sidebar menu with the following items: KVM, Inband, Network (selected), Host Settings, Syslog, Services (expanded), IP Filtering, VPN, SNMP, Host Tables, Static Routes, AUX Port, and System. The main content area displays four checkboxes: Telnet, SSH, SNMP, and IPsec.

By selecting the appropriate box, the Services form allows you to enable or disable the daemons to use to allow different incoming connections.

Note: If you plan on using VPN, make sure to enable IPsec.

Depending on the security requirements of your site, you may want to enable or disable the daemons that support the following types of connections:

- telnet [enabled by default]
- SSH [enabled by default]
- SNMP [enabled by default]
- IPsec

Each of these services is required when telnet, ssh, SNMP, or VPN are configured, as described in the following table.

Service Name	Notes and Where Documented
Telnet	Enable telnet if users need to access the KVM/net through telnet.
SNMP	Enable “SNMP” if you configure SNMP in “To Configure SNMP” on page 231.
IPsec	Enable “IPsec” if you configure VPN in “To Configure VPN” on page 228.

▼ **To Select the Daemons Used for Incoming Connections**

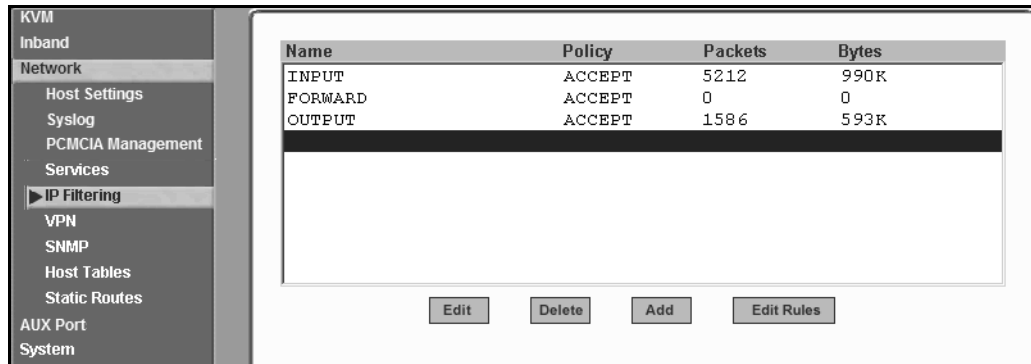
1. In Expert mode got to: Configuration>Network>Services.

The Services form appears.

2. Select or clear the check boxes next to the desired service(s) to enable or disable the service.
3. Select “apply changes” when done.

IP Filtering

Selecting Configure>Network>IP Filtering in Expert mode brings up the IP Filtering form as shown in the following figure.



You can use the IP Filtering form to filter traffic to and from the KVM/net and block traffic according to rules you define.

The KVM/net uses chains and rules for filtering packets like a firewall. Each entry in the list represents a chain with a set of rules.

The form by default has three built-in chains, as shown in the previous figure. The chains accept all INPUT, FORWARD, and OUTPUT packets. You can use the form to do the following to specify packet filtering:

- Add a new chain and specify rules for that chain
- Add new rules
- Delete existing chains and rules.

Add Rule and Edit Rule Options

The Add Rule and Edit Rule dialog boxes have the fields and options shown in the following figure.

The dialog box contains the following elements:

- Buttons: OK, Cancel, Help
- Target: ACCEPT (dropdown menu)
- Source IP: [Text Box] Mask: [Text Box] Inverted
- Destination IP: [Text Box] Mask: [Text Box] Inverted
- Protocol: All (dropdown menu) Inverted
- Input Interface: [Text Box] Inverted
- Output Interface: [Text Box] Inverted
- Fragments: All packets (dropdown menu)

Inverted Check Boxes

If you check the “Inverted” check box on any line, the target action is performed on packets that do not match any of the criteria specified in that line when any other specified criteria are also met.

For example, if you select DROP as the target action, check “Inverted” on the line with a source IP address specified, and do not specify any other criteria in the rule, any packets arriving from any other source IP address than the one specified are dropped.

Target Pull-down Menu Options

The “Target” is the action to be performed on an IP packet that matches all the criteria specified in a rule. The target pull-down menu is shown in the following figure.

The image shows a web form element labeled "Target". It consists of a dropdown menu currently displaying "DROP". The dropdown list is open, showing the following options: "ACCEPT", "DROP" (highlighted), "RETURN", "LOG", and "REJECT".

If the “LOG” and “REJECT” targets are selected, additional fields appear as described under “LOG Target” on page 216 and “REJECT Target” on page 217.

Source or Destination IP and Mask

If you fill in the “Source IP” field, incoming packets are filtered for the specified IP address. If you fill in the “Destination IP” field, outgoing packets are filtered for the specified IP address.

If you fill in either “Mask” field, incoming or outgoing packets are filtered for IP addresses from the network in the specified netmask.

The source and destination IP and related fields are shown in the following figure.

The image shows a form with two rows of input fields. The first row is for "Source IP" and "Mask", and the second row is for "Destination IP" and "Mask". Each row has a text input field followed by a checkbox labeled "Inverted".

Protocol

You can select a protocol for filtering from the “Protocol” pull-down menu, which is shown in the following figure.

The image shows a dropdown menu for "Protocol". The menu is open, showing the following options: "ICMP", "Numeric", "All", "TCP", "UDP", and "ICMP" (highlighted).

The additional fields that appear for each protocol are explained in the following sections.

Numeric Protocol Fields

If you select Numeric as the protocol when specifying a rule, a text field appears to the right of the menu for you to enter the desired number, as shown in the following figure.

TCP Protocol Fields

If you select TCP as the protocol when specifying a rule, the additional fields shown in the following figure appear for you to fill out at the bottom of the form.

The following table defines the fields and menu options in the “TCP Options Section.”

Field/Menu Option	Definition
Source Port - OR - Destination Port -AND- to	You can specify a source or destination port number for filtering in the “Source Port” or “Destination Port” field. If you specify a second number in the “to” field, TCP packets are filtered for any port number within the range that starts with the first port number and that ends with the second.
TCP Flags	You can select the check box next to any of the TCP flags: “SYN” (synchronize), “ACK” (acknowledge), “FIN” (finish), “RST” (reset), “URG” (urgent), or “PSH” (push) and select either “Any,” “Set,” or “Unset,” TCP packets are filtered for the specified flag and the selected condition.

UDP Protocol Fields

If you select UDP as a protocol when specifying a rule, the additional fields shown in the following figure appear at the bottom of the form.

UDP Options Section

Source Port to Inverted

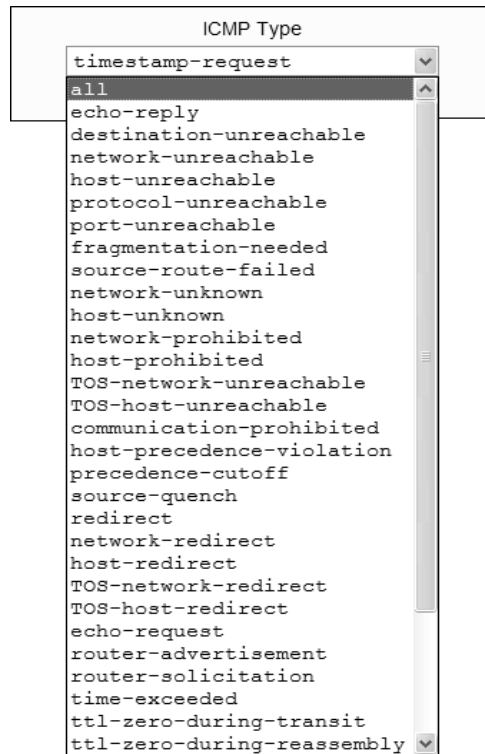
Destination Port to Inverted

The following table defines the fields in the UDP Options Section.

Field	Definition
<p>Source Port - OR - Destination Port -AND- to</p>	<p>Specify a source or destination port number for filtering in the “Source Port” or “Destination Port” field.</p> <p>You can specify a source or destination port number for filtering in the “Source Port” field. If you specify a second number in the “to” field, TCP packets are filtered for any port number within the range that starts with the first port number and that ends with the second.</p>

ICMP Protocol Fields

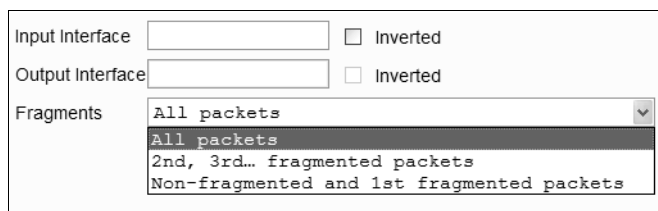
If you select ICMP as a protocol when specifying a rule, the ICMP Type pull-down menu appears in the ICMP Options Section at the bottom of the IP Filtering form. The following figure shows the options.



Input Interface, Output Interface, and Fragments

If you enter an interface (such as eth0 or eth1) in the “Input Interface” field, incoming packets are filtered for the specified interface. If you enter an interface in the “Output Interface” field, outgoing packets are filtered for the specified interface.

These fields are shown in the following figure.



The following table defines the fields in the previous figure.

Field	Definition
Input Interface	The input interface (eth N) for the packet
Output Interface	The output interface (eth N) for the packet
Fragments	The types of packets to be filtered: All packets 2nd, 3rd... fragmented packets Non-fragmented and 1st fragmented packets

LOG Target

If you select “LOG” from the “Target” field, the following fields and menus appear in the “LOG Options Section” at the bottom of the form.

LOG Options Section

Log Level Log Prefix

TCP sequence TCP options IP options

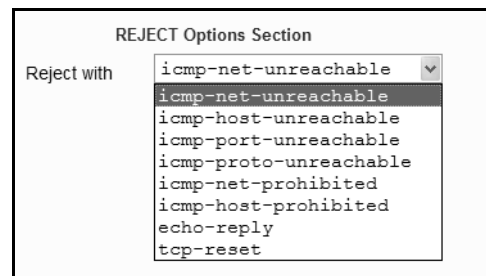
The following table defines the menu options, field, and check boxes in the “LOG Options Section.”

Field or Menu Name	Definition
Log Level	One of the options in the pull-down menu: <div style="border: 1px solid black; padding: 5px; margin: 5px 0;"> emerg ▼ emerg alert crit err warning notice info debug </div>
Log Prefix	The prefix to use in the log entry.

Field or Menu Name	Definition
TCP Sequence	Checking the box includes the TCP sequence in the log.
TCP Options	Checking the box includes TCP options in the log.
IP Options	Checking the box includes IP options in the log.

REJECT Target

If you select REJECT from the Target pull-down menu, the following pull-down menu appears



Any “Reject with” option causes the input packet to be dropped and a reply packet of the specified type to be sent.

Firewall Configuration Procedures

The following table has links to the procedures for defining packet filtering:

To Add a Chain [Expert]	Page 218
To Edit a Chain [Expert]	Page 218
To Edit a Rule for IP Filtering	Page 219
To Add a Packet Filtering Rule [Expert]	Page 220

▼ **To Add a Chain [Expert]**

1. Go to Configuration>Network >Firewall Configuration in Expert Mode.
The IP Filtering form appears.
2. Click “Add.”
The “Add Chain” dialog box appears.



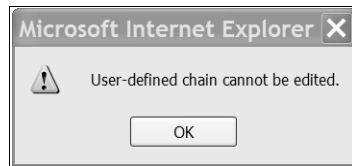
3. Enter the name of the chain to be added in the “Name” field and then click OK.
Spaces are not allowed in the chain name.
The name of the new chain appears in the list.
4. Finish defining the chain by adding one or more rules, as described in to “To Add a Rule” on page 245.

▼ **To Edit a Chain [Expert]**

Perform this procedure if you want to change the policy for a default chain.

Note:User-defined chains cannot be edited.

1. Go to Configuration>Network >Firewall Configuration in Expert Mode.
2. Select one of the default chains from Chain list, and then click the “Edit” button.
If you select a user-defined chain, the following dialog box appears.



If you select one of the default chains, the “Edit Chain” dialog box appears.



3. Select the desired policy from the Policy pull-down menu, and then click OK.
4. Click “apply changes.”
5. To edit any rules for this chain, go to “To Edit a Rule.”

▼ **To Edit a Rule for IP Filtering**

1. In Expert mode go to: Configuration > Network > IP Filtering.

The IP Filtering configuration form appears.

See “To Add a Rule for IP Filtering” on page 222 procedure section for a definition of the user input fields.

2. Select a chain whose rule you want to edit.

3. Click the Edit Rule button.

The Edit Rules form appears. Each line represents a rule for the selected chain.

4. Select the Chain you wish to edit from the Chain list, and click the Edit Rule button.

The Edit Rules form appears.

5. Specify the rule as desired.
See “IP Filtering” on page 210 for a definition of the input fields, if needed.
6. Click on the “apply changes” button to complete the procedure.

▼ **To Add a Packet Filtering Rule [Expert]**

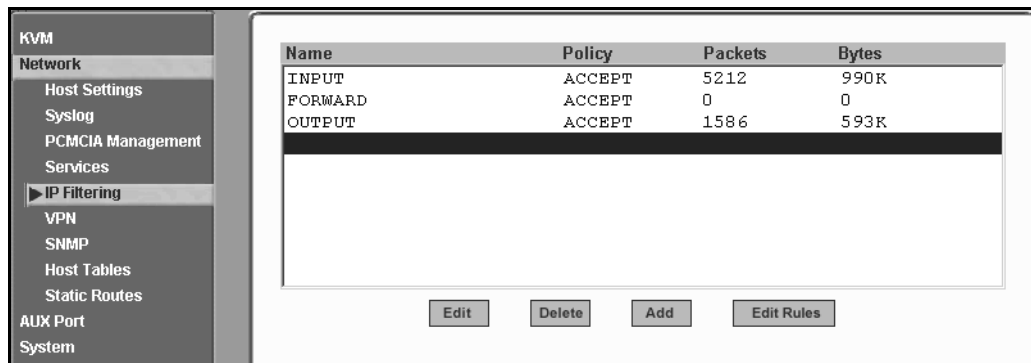
1. Go to Configuration>Network >Firewall Configuration in Expert Mode.
2. Select the chain whose rule you want to edit from Chain list, and then and then click the “Edit Rules” button.
3. Click the “Edit Rule” button.
The “Edit Rule for Chain” dialog box appears.
4. Specify the rule as desired.
5. Click the “Add” button.
The “Add Rule” dialog box appears.
6. Complete the Add Rule dialog box.
7. Click “apply changes.”

You can perform the following task from the IP Filtering Form:

- “To Add a Chain for IP Filtering” on page 220
- “To Edit A Chain for IP Filtering” on page 222
- “To Add a Rule for IP Filtering” on page 222
- “To Edit a Rule for IP Filtering” on page 219

▼ **To Add a Chain for IP Filtering**

1. In Expert mode go to: Configuration > Network > IP Filtering.
The IP Filtering configuration form appears.



Name	Policy	Packets	Bytes
INPUT	ACCEPT	5212	990K
FORWARD	ACCEPT	0	0
OUTPUT	ACCEPT	1586	593K

Each line in the list box represents a chain. For a definition or explanation of the field columns, refer to the introductory section of this procedure or to the field definitions for the Edit Rule dialog box, next section.

2. To add a chain, select the Add button.

The Add Chain dialog box appears.



3. Enter the name of the chain that you are adding to the filter table, and then select OK. (Spaces are not allowed in the chain name.)
4. After entering a new chain name, click on the Edit Rules button to enter the rules for that chain.
5. Select OK to commit your changes.
6. To add rules to your new chain, see “To Add a Rule for IP Filtering” on page 222.

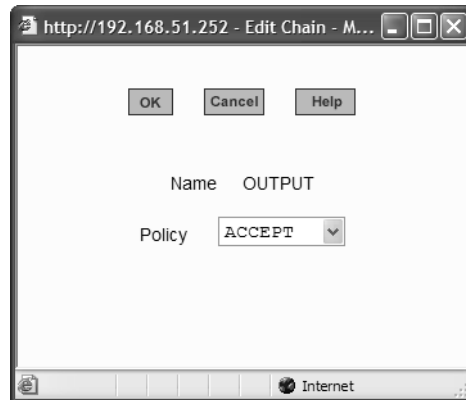
▼ **To Edit A Chain for IP Filtering**

1. In Expert mode go to: Configuration > Network > IP Filtering.

The IP Filtering configuration form appears.

2. Select the Chain you wish to edit from the Chain list box (or filter table), and select the Edit button.

The Edit Chain dialog box appears.

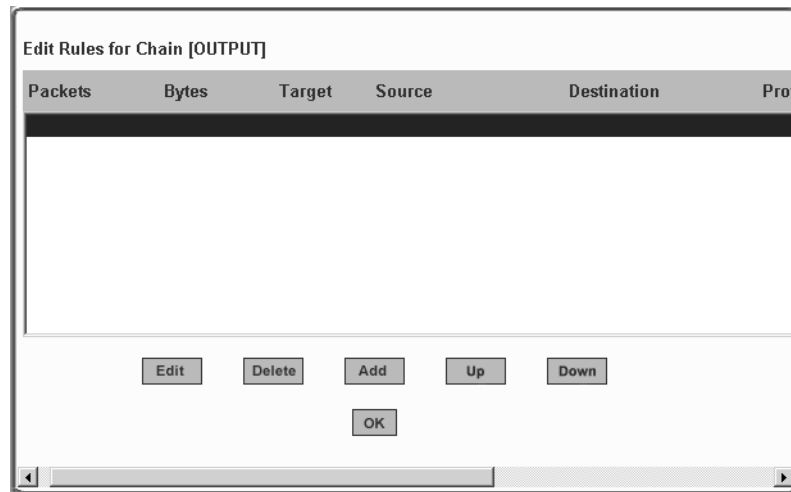


3. Modify the Policy field, as needed, and select OK.
4. Verify your entry from the main form and click “apply changes” to save your changes.
5. If you need to add any rules for this chain, go to “To Add a Rule for IP Filtering” on page 222.

▼ **To Add a Rule for IP Filtering**

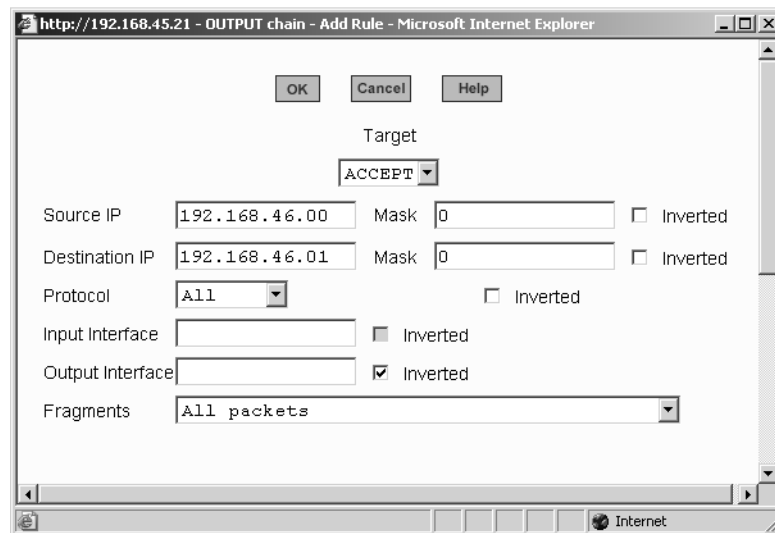
1. In Expert mode go to: Configuration > Network > IP Filtering.

The IP Filtering configuration form appears.



2. Click the Add button.

The Add Rule dialog box appears.



3. Complete the following data fields as necessary:

Field Name	Definition
Target	Indicates the action to be performed to the IP packet when it matches the rule. For example, the kernel can ACCEPT DROP, RETURN, LOG or REJECT the packet by sending a message, translating the source or the destination IP address/port or sending the packet to another user-defined chain.
Source IP	The source IP address.
Mask	Source network mask. Required when a network should be included in the rule.
Inverted	Select the check box adjacent to Source IP to invert the target action. For example, the action assigned to the target will be performed to all source IPs/Masks except to the one just defined.
Destination IP	Destination IP address.
Mask	Destination network mask.
Inverted	Select the check box adjacent to Destination IP to invert the target action. For example, the action assigned to the target will be performed to all Destination/Mask IPs except to the one just defined.
Protocol	The transport protocol to check. If the numeric value is available, select Numeric and type the value in the adjacent field; otherwise, select one of the other options.

Field Name	Definition
Inverted	Select the check box adjacent to Protocol to invert the target action. For example, the action assigned to the target will be performed to all protocols except to the one just defined.
Input Interface	The interface where the IP packet should pass. The Input Interface option appears only for the INPUT and FORWARD chains.
Inverted	Select the check box adjacent to Input Interface to invert the target action. For example, the action assigned to the target will be performed to all interfaces except to the one just defined.
Output Interface	The interface where the IP packet should pass. The Output interface option will appear for the chains FORWARD and OUTPUT.
Inverted	Select box adjacent to Output Interface to invert the target action. For example, the action assigned to the target will be performed to all interfaces except to the one just defined.
Fragments	Indicates the fragments or unfragmented packets to be checked. The IP Tables can check for: <ul style="list-style-type: none"> <li data-bbox="797 1419 954 1451">• All Packets <li data-bbox="797 1472 1179 1503">• 2nd, 3rd... fragmented packets <li data-bbox="797 1524 1247 1581">• Non-fragmented and 1st fragmented packets
ICMP Type	This dropdown list box contains all the ICMP types that may be applied to the current rule.

Field Name	Definition
Inverted	This ICMP option will be applied to all rules except the currently selected rule.

4. Complete the following additional fields as necessary:

- If you selected Log from the Target field, the following options also appear.

LOG Options Section

Log Level Log Prefix

TCP sequence
 TCP options
 IP options

Field Name	Definition
Log Level	The log level classification to be used based on the type of error message (such as, alert, warning, info, debug, and so on.).
Log Prefix	The prefix that will identify the log.
TCP Sequence	Check box to include TCP sequence in the log.
TCP Options	Check box to include TCP options in the log.
IP Options	Check box to include IP options in the log.

- If you selected Reject from the Target field, the following field appears:

REJECT Options Section

Reject with

- icmp-net-unreachable
- icmp-host-unreachable
- icmp-port-unreachable
- icmp-proto-unreachable
- icmp-net-prohibited
- icmp-host-prohibited
- echo-reply
- tcp-reset

“Reject with” means that the filter drops the input packet and sends back a reply packet according to any of the reject types listed below.

Using tcp flags and appropriate reject type, the packets are matched with the REJECT target. The following options are available:

- icmp-net-unreachable – ICMP network unreachable alias
- icmp-host-unreachable – ICMP host unreachable alias
- icmp-port-unreachable – ICMP port unreachable alias
- icmp-proto-unreachable – ICMP protocol unreachable alias
- icmp-net-prohibited – ICMP network prohibited alias
- icmp-host-prohibited – ICMP host prohibited alias
- echo-reply – Echo reply alias
- tcp-reset – TCP RST packet alias

5. Click on the OK button when done.

6. Click on “apply changes.”

VPN

When VPN Connections is selected under Configuration>Network in Expert mode, you can configure one or more VPN connections.

Selecting one of the existing VPN connections and clicking the edit button or the add button launches a dialog box to prompt for the details of the connection. Complete the fields in the dialog box. The RSA keys may be entered using the Copy and Paste feature of your Browser.

A VPN, or Virtual Private Network lets the KVM/net and a whole network communicate securely when the only connection between them is over a third network which is untrustable. A gateway must exist on the remote network that is capable of encrypting packets going to the KVM/net and decrypting packets from the KVM/net. This creates a security tunnel between the KVM/net and the gateway. The gateway machine and the KVM/net encrypt packets entering the untrusted net and decrypt packets leaving it, creating a secure tunnel through it.

Often it may be useful to have explicitly configured IPsec tunnels between the KVM/net and a gateway of an office with a fixed IP address (in this case every machine on the office network would have a secure connection with the KVM/net), or between the KVM/net and the KVM/net administrator machine, which must, in this case, have a fixed IP address. You can add this

Web Manager for Administrators

connection descriptor to both the Console Server and the other end. This is the advantage of using left and right instead of using local remote parameters.

If you give an explicit IP address for left (and left and right are not directly connected), then you must specify leftnextthop (the router which KVM/net sends packets to in order to get them delivered to right). Similarly, you may need to specify rightnextthop (vice versa).

▼ To Configure VPN

For the VPN to function properly, ensure that you have also enabled IPsec on the Services form. See “To Select the Daemons Used for Incoming Connections” on page 210 for instructions on configuring IPsec.

1. In Expert mode, go to: Configure > Network > VPN.

The VPN form appears.

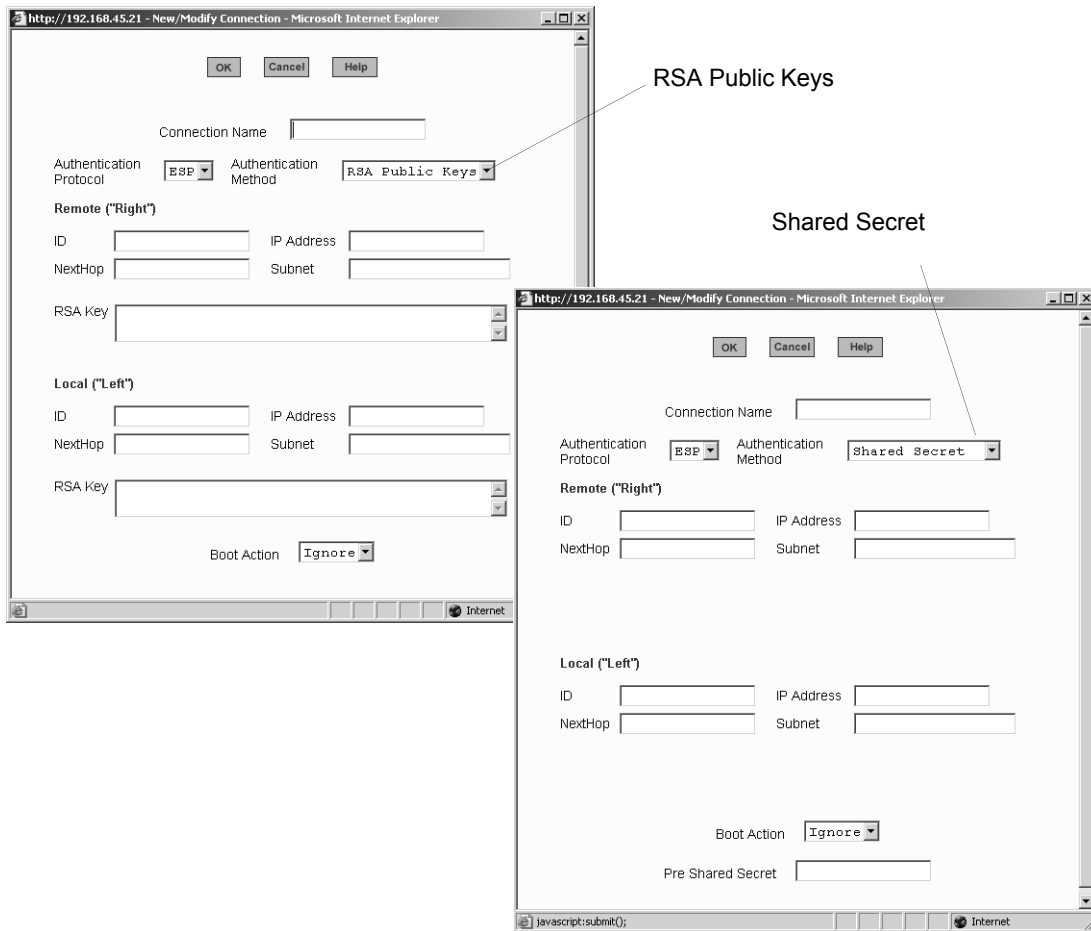


2. To edit a VPN connection, select the VPN connection that you wish to edit from the form, and then select the Edit button.

- OR -

To add a VPN Connection, select the Add button.

The New/Modify Connection dialog box appears.



Note: If the selected authentication method is RSA Public Keys, the dialog box on the left of the previous figure is used; if the authentication method is Shared Secret, the dialog box on the right is used.

3. Edit or complete the appropriate fields as follows.

Field Name	Definition
Connector Name	Name of the VPN connection.

Field Name	Definition
Authentication Protocol	Authentication protocol used to establish a VPN connection.
Authentication Method	Authentication method used to establish a VPN connection.
Remote ("Right")	
ID	The identification name of the remote host, commonly referred to as the "right" host.
IP Address	Remote IP address.
NextHop	The router to which the Console Server sends packets in order to deliver them to the left.
Subnet Mask	As indicated.
RSA Key	You may use the copy and paste feature of your browser to enter the RSA key.
Local ("Left")	
ID	The identification name of the local host, commonly referred to as the "left" host.
IP Address	The IP address of the local or left host.
NextHop	The router to which the Console Server sends packets in order to deliver them to the right.
Subnet Mask	As indicated
RSA Key	You may use the copy and paste feature of your browser to enter the RSA key.
Boot Action	The boot action configured for the local host.

Field Name	Definition
Pre-Shared Secret	Pre-shared password between left and right users.

4. Select the OK button when done.
5. Select the “apply changes” button to save your configuration.

SNMP

Short for Simple Network Management Protocol, SNMP is a set of protocols for managing network devices. SNMP works by sending messages, called protocol data units (PDUs), to different parts of a network. SNMP-compliant devices (*agents*), store data about themselves in Management Information Bases (MIBs) and return this data to the SNMP requesters.

The KVM/net uses the Net-SNMP package (<http://www.net-snmp.org/>). The Net-SNMP package contains various tools relating to the Simple Network Management Protocol including an extensible agent, an SNMP library, tools to request or set information from SNMP agents, tools to generate and handle SNMP traps, a version of the unix 'netstat' command using SNMP, and a Tk/Perl mib browser.

SNMP is configured with community names, OID and user names. The KVM/net supports SNMP v1, v2, and v3. The two versions require different configurations. SNMP v1/v2 requires community, source, object ID and the type of community (read-write, read-only). V3 requires user name.

Important: Check the SNMP configuration before gathering information about KVM/net by SNMP. An unauthorized user can implement different types of attacks to retrieve sensitive information contained in the MIB. By default, the SNMP configuration in KVM/net cannot permit the public community to read SNMP information.

▼ **To Configure SNMP**

1. In Expert Mode go to: Configuration > Networks > SNMP.

The SNMP form appears.

Web Manager for Administrators

To activate the snmpd services, you should go to the Network Services section.

System Information Settings

SysContact

SysLocation

Access Control

SNMPv1/SNMPv2 Configuration

Community	Source	OID	Permission

SNMPv3 Configuration

User name	Permission	OID

2. Enter the following system information, as necessary:

Field Name	Definition
Community	The community name acts as a password to authenticate messages sent between an SNMP client and a router containing an SNMP server. The community name is sent in every packet between the client and the server.
SysContact	The email of the person to contact regarding the host on which the agent is running (e.g., me@mymachine.mydomain)
SysLocation	The physical location of the system (e.g., mydomain).

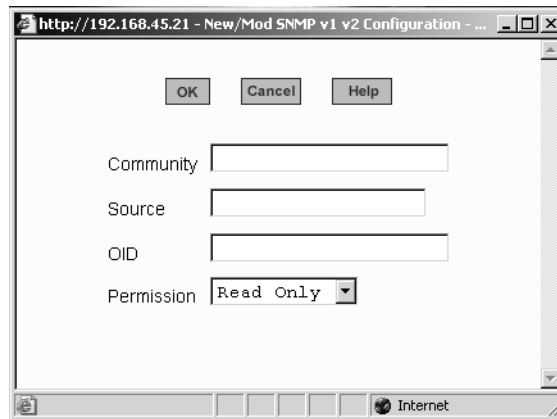
If you are using SNMPv3, skip to [Step 6](#).

3. To Add an SNMP agent using SNMPv1/SNMP2 Configuration, select the Add button located at the bottom of this view table.

OR

To edit an SNMP agent, select the Edit button.

The New/Modify SNMP Daemon Configuration dialog box appears.

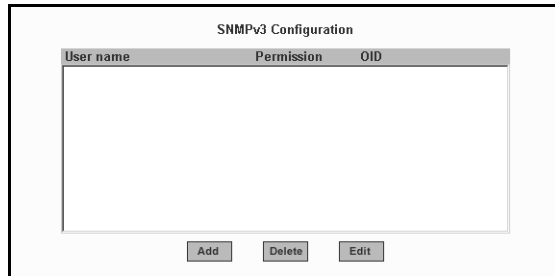


4. Complete the dialog box as follows:

Field Name	Definition
Community	The community name acts as a password to authenticate messages sent between an SNMP client and a router containing an SNMP server. The community name is sent in every packet between the client and the server.
Source	The source IP address or range of IP address.
OID	Object Identifier.

Field Name	Definition
Permission	Select the permission type: <ul style="list-style-type: none"> • Read Only – Read-only access to the entire MIB except for SNMP configuration objects. • Read/Write – Read-write access to the entire MIB except for SNMP configuration objects. • Admin – Read-write access to the entire MIB.

5. If you are adding or editing an SNMP agent using SNMPv3, scroll down to the lower half of the SNMP Configuration form and select the Add button located at the bottom of this view table



6. To add an SNMP agent using SNMPv3, click Add.

7. To edit an SNMP agent using SNMPv3, click Edit.

The New/Modify SNMP Daemon Configuration dialog box.



8. Complete the form and when done.

Field Name	Definition
Username	Name of user account accessing the KVM/net Plus.
Source	The source IP address or range of IP address.
OID	Object Identifier.
Permission	Select the permission type: <ul style="list-style-type: none"> • Read Only – Read-only access to the entire MIB except for SNMP configuration objects. • Read/Write – Read-write access to the entire MIB except for SNMP configuration objects.

9. Click the OK button.

10. Verify your entry or modification on the SNMP form.

11. Click “apply changes” to complete the procedure.

Host Tables

The Host Tables form enables you to keep a table of host names and IP addresses that comprise your local network, and thus provide information about your network environment.

▼ To Configure Hosts

1. In Expert Mode, go to: Configuration>Network>Host Tables.

The Host Tables form appears.

Web Manager for Administrators



2. Do on of the following:

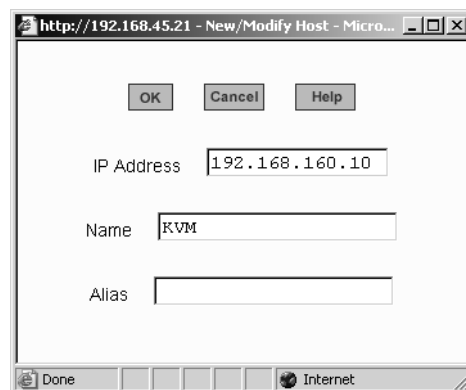
- To edit a host, select the host IP address from the Host Table and then click the Edit button.

If the list is long, use the Up and Down buttons to go through each item in the list.

- OR -

- To add a host, click the Add button.

The New/Modify Host dialog box appears.



3. Enter the new or modified host address in the IP Address field and the host name in the Name field.
4. Click the OK button.
5. To delete a host, select the host you wish to delete from the Host Table form, and select the Delete button on the form.
6. Select “apply changes” to save your configuration to Flash.

Static Routes

The Static Routes form allows you to manually add routes. The Routing Table defines which interface should transmit an IP packet based on destination IP information. Static routes are a quick and effective way to route data from one subnet to another.

To Add, Edit, or Delete a Static Route

1. In Expert mode, go to: Configure > Network > Static Routes.

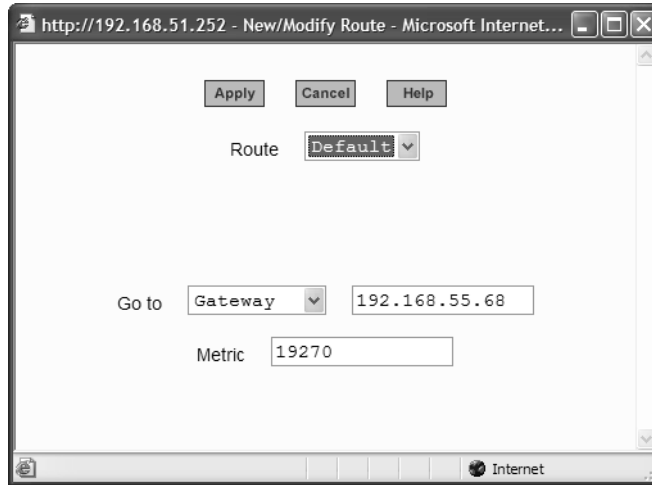
The Static Routes table form appears.



2. Do one of the following:
 - To edit a static route, select a route from the Static Routes form, and click the Edit button.

Web Manager for Administrators

- To add a static route, select the Add button from the form. The New/Modify Route dialog box appears.



3. Complete the dialog box as follows:

Table 4-3: Add/Modify Static Routes Fields

Field Name	Definition
Route	Select Default, Network, or Host.
Network IP	The address of the destination network. This field appears only if Network is selected.
Network Mask	The mask of the destination network. This field appears only if Network is selected.
Host IP	The IP address of the destination host. This field appears only if Host is selected.
Go to	Select Gateway or Interface.
Field Adjacent to Go to	The address of the gateway or interface.

Table 4-3: Add/Modify Static Routes Fields

Field Name	Definition
Metric	The number of hops.

4. Click the Apply button to close the dialog box.
The new or modified route appears in the list.
5. To delete a static route, select a route from the list and click Delete.
6. Click “apply changes.”

AUX Port

Selecting Configuration>AUX Port in Expert mode brings up the following form.

The screenshot displays the 'AUX Port' configuration page in the 'cyclades' web interface. The page is titled 'Access | Configuration | Information | Management' and shows the user's host name as 'ana-kvm' with IP address '192.168.51.16' and model 'KVM/net 16'. The left sidebar contains a 'Wizard' button and a navigation menu with 'KVM', 'Inband', 'Network', 'AUX Port', and 'System'. The main content area is a configuration form for the AUX port. It features a 'Profile' dropdown set to 'PPP', a 'Baud Rate (Kbps)' dropdown set to '9600', 'Flow Control' set to 'None', 'Data Size' set to '8', 'Parity' set to 'None', and 'Stop Bits' set to '1'. The 'Modem Initialization' field contains the text: 'TIMEOUT 10', '\d\vdATZ', and 'OK\r\n-ATZ-OK\r\n'. Below these are input fields for 'Local IP address' and 'Remote IP address', and a checked checkbox for 'Authentication Required'. At the bottom of the form, there is a 'Wizard' button and a toolbar with icons for 'try changes', 'cancel changes', 'apply changes', 'reload page', 'Help', and 'no unsaved changes'.

The AUX Port form is used to configure the AUX port for use with an AlterPath PM or an external modem or an external modem.

▼ **To Configure the AUX Port for Use With a PM or an External Modem**

1. In Expert mode go to: Configuration > AUX Port.

The Aux Port form appears.

2. To configure the AUX port for Power Management, make sure that Power Management is selected in the Profile drop-down list.

The image shows a web form with a label 'Profile:' followed by a dropdown menu. The dropdown menu is open, displaying three options: 'Power Management' (which is highlighted with a dark background), 'Power Management', and 'PPP'.

3. Click “apply changes.”

See “Power Management” on page 41 for background information on power management and lists of related tasks.

4. To configure the AUX port for an external modem, make sure that PPP is selected in the Profile field.

Additional fields appear on the form.

5. Complete the fields as shown below.

Table 4-4: PPP Fields for Configuring the AUX Port

Field Name	Definition
Profile	Select the device to be connected. For PPP , the following input fields are used:
Baud Rate	The port speed.
Flow Control	Gateway or interface address used for the route.
Data Size	The number of data bits.
Parity	None, even or odd.
Stop Bits	The number of stop bits.
Modem Initialization	The modem initialization string.

Table 4-4: PPP Fields for Configuring the AUX Port (Continued)

Field Name	Definition
Local IP Address	The IP address of the KVM/net.
Remote IP Address	The remote IP address
Authentication Required	Select check box if authentication is required.
MTU/MRU	The maximum transmission unit / maximum receive units for the PPP.
PPP Options	The options for this protocol.

6. Click “apply changes.”

System

Selecting Configuration>System in Expert mode brings up the System form as shown in the following figure.

The screenshot shows the 'System' configuration page in the cyclades web interface. The page is titled 'System' and is part of the 'Configuration' section. The interface includes a navigation menu on the left with options like 'KVM', 'Inband', 'Network', 'AUX Ports', 'System', 'Time / Date', and 'Boot Configuration'. The main content area displays the following configuration fields:

- Timezone: GMT (dropdown menu)
- Network Time Protocol: Disable (dropdown menu)
- Date:
 - Month: 6
 - Day: 15
 - Year: 2005
- Time:
 - Hour: 19
 - Minute: 55
 - Second: 46

The bottom toolbar contains buttons for 'try changes', 'cancel changes', 'apply changes', 'reload page', 'Help', and 'no unsaved changes'. The top right corner shows 'logout' and system information: 'Host Name: KVM', 'IP Address: 192.168.51.252', and 'Model: KVM/net Plus 32'.

Web Manager for Administrators

The screenshot displays the Cyclades Web Manager interface for administrators. The top navigation bar includes 'Access | Configuration | Information | Management' and a 'logout' link. The host information is shown as 'Host Name: ana-kvm', 'IP Address: 192.168.51.16', and 'Model: KVM/net 16'. The left sidebar lists navigation options: 'KVM', 'Inband', 'Network', 'AUX Port', 'System', 'Time / Date', and 'Boot Configuration'. The main content area is titled 'Timezone' and 'Network Time Protocol', with 'GMT' selected for the Timezone and 'Disable' for the Network Time Protocol. Below this, there are input fields for 'Date' (Month: 6, Day: 15, Year: 2005) and 'Time' (Hour: 19, Minute: 55, Second: 46). At the bottom, there are buttons for 'Wizard', 'try changes', 'cancel changes', 'apply changes', 'reload page', 'Help', and 'no unsaved changes'.

With the System form administrators can set the time and date on the KVM/net and reboot the KVM/net if necessary. The following procedures are available on the System form:

- “To Set the KVM/net’s Date and Time Manually” on page 243
- “To Set The Time and Date With NTP” on page 243
- “To Set the Time and Date to the KVM/net’s Local GMT” on page 244
- “To Configure KVM/net Boot” on page 248

Time/Date

With the Time/Date form, you have three options for setting the time and date of your system:

- “To Set the KVM/net’s Date and Time Manually” on page 243
- “To Set The Time and Date With NTP” on page 243
- “To Set the Time and Date to the KVM/net’s Local GMT” on page 244

KVM
Network
AUX Port
System
Time / Date
Boot Configuration

Enable Timezone: GMT

Network Time Protocol: Disable

Date

Month 2 Day 17 Year 2005

Time

Hour 11 Minute 35 Second 37

▼ To Set the KVM/net's Date and Time Manually

1. In Expert Mode, go to: Configuration > System > Time/Date.

The Date/Time form appears.

2. Make sure that Disabled is selected in the Network Time Protocol drop-down list.

Network Time Protocol: Disable

Date

Month 2 Day 16 Year 2005

Time

Hour 16 Minute 29 Second 5

3. Fill in the date and time fields by selecting the appropriate numbers from the drop-down lists.
4. Click “apply changes.”

▼ To Set The Time and Date With NTP

1. In Expert Mode, go to: Configuration > System > Time/Date.

The Date/Time form appears.

2. Choose Enable from the Network Time Protocol drop-down list.

The NTP Server field appears.

Web Manager for Administrators

Enable Timezone: GMT
Network Time Protocol: Enable
NTP Server: 129.6.15.28

3. Enter the address of the NTP server in the NTP Server field.
4. Click the “apply changes” button.

▼ **To Set the Time and Date to the KVM/net’s Local GMT**

1. Select Administration from the top menu bar.
2. Select Time/Date from the left menu panel.

The Time/Date form appears.

3. Select the appropriate GMT from the Timezone drop-down list. Only official time zones are available.

Enable Timezone: GMT
GMT
GMT 1 h West
GMT 2 h West
GMT 3 h West
GMT 4 h West
GMT 5 h West
GMT 6 h West
GMT 7 h West
GMT 8 h West
GMT 9 h West
GMT 10 h West

4. Click “apply changes.”

Boot Configuration

Selecting Configuration>System>Boot Configuration brings up the following form.

The screenshot shows the Cyclades web interface for KVM configuration. The main content area is titled "Boot Configuration" and contains the following fields:

- IP Address assigned to Ethernet: 192.168.160.10
- Watchdog Timer: Active
- Unit boot from: image1: vmlinux.UBoot.0414_ga
- Boot File Name: zmpckvmp.bin
- Server's IP Address: 192.168.160.1
- Console Speed: 9600
- Fast Ethernet: Auto Negotiation
- Fast Ethernet Max Interrupt Events: 0

At the bottom of the form, there are several buttons: "Wizard", "try changes", "cancel changes", "apply changes", "reload page", "Help", and "no unsaved changes".

On the Boot Configuration form, you can redefine the location from which the KVM/net boots.

By default, the KVM/net boots from a boot file in the on-board Flash memory. To understand the “Unit boot from” options, you need to understand how the KVM/net handles software upgrades:

- The KVM/net initially boots from a software image referred to as “image1.”
- The first time you download and install a new software version from Cyclades, the new image is stored as “image2” in the Flash memory and the configuration is changed to boot the KVM/net from “image 2.”
- The second time you download a new software version, the latest image is stored as “image 1,” and the KVM/net configuration is changed to boot from “image1.”
- Subsequent downloads are stored following the same pattern, alternating “image1” with “image2.”

In the “Unit boot from” pull-down menu, an entry showing the number of the *current* image and the name of the boot file are selected by default. The word “image” is followed by the number, followed by a colon (:), followed by the name of the file, including the version number. In the initial configuration, the menu item appears as follows:

Web Manager for Administrators

image1: zvmppcons.vversion_number

For the first version the filename would be:

image1: zvmppcons.v100

After one or more software upgrades have been performed, a second image is also listed in the menu, for example:

image1: zvmppcons.v100

image2: zvmppcons.v101

If, for any reason, you want to boot from another image than the one currently selected, you can select that image from the “Unit boot from” menu. You can select “Network” and configure a boot server to boot from the network instead, if desired.

A network boot has the following prerequisites:

- A TFTP or BOOTP server must be available to the KVM/net on the network.
- An upgraded KVM/net boot image file must be downloaded from Cyclades and available on the boot server.
- The KVM/net must have a fixed IP address and you must know the address.
- You must know the boot filename and the IP address of the TFTP server.

These and other boot related options are described in the following table.

Table 4-5: Boot Configuration Fields and Options

Field or Value Name	Description
IP Address assigned to Ethernet	A new IP address for the KVM/net.
Watchdog Timer	Whether the watchdog timer is active. If the watchdog timer is active the KVM/net reboots if the software crashes. See “Boot Configuration” on page 286 for how the watchdog timer can be activated or deactivated.
Unit boot from	Choose one or more images and “Network” from the list.

Table 4-5: Boot Configuration Fields and Options (Continued)

Field or Value Name	Description
Boot File Name	An alternative name for the boot file.
Server's IP Address	An IP address for a boot server.
Console Speed	An alternative console speed from 4800 to 115200 (9600 is the default).
Fast Ethernet	The speed of the Ethernet connection: Auto Negotiation, 100 BaseT Half-Duplex, 100 BaseT Full-Duplex, 10 BaseT Half-Duplex, 10 BaseT Full-Duplex
Fast Ethernet Max Interrupt Events	An alternate number of maximum interrupt events to improve performance (0 is the default)

▼ **To Configure KVM/net Boot**

For more information about the fields in the “Boot Configuration” form, see Table 4-5 on page 246, if desired.

1. Go to Configuration > System > Boot Configuration in Expert mode.
The Boot Configuration form appears.
2. Enter the IP address of the KVM/net in the “IP Address assigned to Ethernet” field.
3. Accept or change the selected option in the “Watchdog Timer” field.
4. Choose the desired image or “Network” from the “Unit boot from” menu.
5. Accept or change the filename of the boot program in the “Boot File Name” field.
6. If specifying network boot, do the following steps.
 - a. Enter the IP address of the tftp server in the “Server’s IP Address” field.
 - b. Select a console speed to match the speed of the tftp server from the “Console Speed” pull-down menu.
 - c. Choose an Ethernet speed from the “Fast Ethernet” pull-down menu.
 - d. Specify the maximum number of packets that the CPU handles before an interrupt in the “Fast Ethernet Max. Interrupt Events” field.
7. Click “apply changes.”

Viewing System Information

The Information menu provides three forms for viewing information about your KVM/net:

- General
- Port Status
- Read Sensor

General

Use the General form to view system information in the following categories:

- System – Kernel version, date, uptime, power supply
- CPU – CPU, clock, revision, Bogomips
- Memory – Total, free, cached, active/inactive, and so on.
- Ram Disk Usage – 1k-blocks, used/available, percent used, and mounted
- Fan Status – Rotations per minute

▼ **To View General Information for Your KVM/net**

1. In Expert mode, go to: Information>General.

The General information form appears.



Port Status

Use the Port Status form to view the system status of each KVM/net port. The Port Status form displays information for six ports—two local and four remote.

Note: Remote port status does not appear on the Port Status form unless one or more remote ports is configured in the system.

▼ To View Port Status

1. In Expert mode, go to: Information > Port Status.
The Port Status form appears.



The following table describes the information displayed for each port on the Port Status form.

Table 4-6: Port Status Information

Field	Information
Station	Displays whether the station is Local, Remote, or Inactive and lists the microcontroller version used. This field also displays whether the KVM/net is a Master or Slave and lists the model number of the master KVM/net.
Connection mode	Displays whether the connection is Network or Physical or if the system is Trying to connect (if the cable is disconnected).
Current status	Displays the name of the current active page for that session.
Login	If a user is logged in, displays the user name and duration of the session in seconds.
Current server	When connected to a port, displays the server name.

Table 4-6: Port Status Information

Field	Information
Connection status	When connected to a port, displays the type of switch, expander, and version number used.
Current permissions	When connected to a port, displays the permissions the current user has on that port.
Cycle	When connected to a port and in Cycle Mode, this field displays the time in seconds that the system has been cycling.

Management

Selecting Management in Expert mode brings up the Management form as displayed in the following figure.

The screenshot shows the 'Management' section of the Cyclades web interface. On the left is a sidebar with the following menu items: Backup Configuration, Firmware Upgrade, Microcode Upgrade, Microcode Reset, Active Sessions, and Reboot. The main content area contains a form with the following elements:

- A 'Type' dropdown menu currently showing 'FTP'.
- Input fields for 'Server IP', 'Path and Filename', 'Username', and 'Password'.
- 'Save' and 'Load' buttons below the input fields.

At the bottom of the interface, there is a 'Wizard' button and a row of control buttons: 'try changes', 'cancel changes', 'apply changes', 'reload page', 'Help', and 'no unsaved changes'.

Administrators can use the management menu to perform system and software management such as booting, backing up, upgrading firmware, and handling configuration data.

Menu Selection	Use this menu to:
Backup Configuration	Use a FTP server to save or retrieve your configuration data.
Firmware Upgrade	Upload firmware from the web to the KVM/net and save the new software version or update.
Microcode Upgrade	Update any of the microcontroller microcodes that are stored in the KVM terminator, main KVM/net, local KVM/net, and internal KVM/net switch.
Microcode Reset	Reset any of the micro controller microcodes.
Active Sessions	View the status of all active sessions as well as reset or kill sessions.
Reboot	Reboot the system.

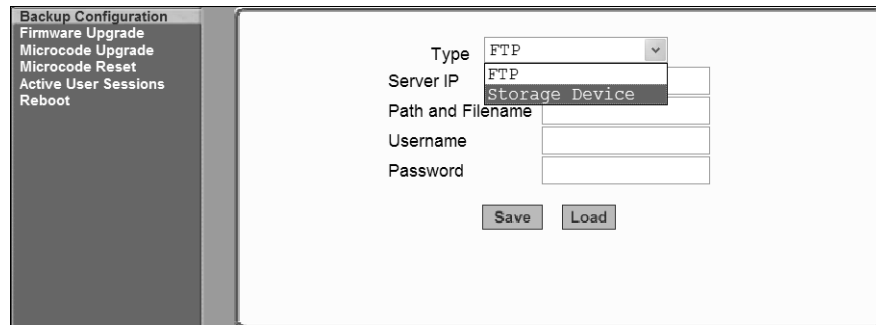
Backup Configuration

The Backup Configuration form allows you to set the KVM/net to use an FTP server to save and retrieve its configuration data.

For the backup configuration to work, the FTP server must be on the same subnet as the KVM/net. Ping the FTP server, to ensure that it is accessible from the KVM/net.

Selecting Management>Backup Configuration in Expert mode brings up the form shown in the following figure.

Web Manager for Administrators



The screenshot shows a web interface for configuration. On the left is a vertical menu with the following items: Backup Configuration (highlighted), Firmware Upgrade, Microcode Upgrade, Microcode Reset, Active User Sessions, and Reboot. The main content area contains a form with the following fields: a 'Type' dropdown menu with 'FTP' selected, a 'Server IP' text input field, a 'Path and Filename' text input field, a 'Username' text input field, and a 'Password' text input field. At the bottom of the form are two buttons: 'Save' and 'Load'.

You can use the form to specify an FTP server for saving the KVM/net configuration, so you can retrieve the configuration if it is ever erased. You can also use the form for retrieving a copy of the backed up configuration file from the FTP server.

The FTP server must be on the same subnet. Ensure that it is accessible by pinging the FTP server.

The following table described the information you need to enter in the fields on the “Backup Configuration” form when FTP is selected from the “Type” pull-down menu.

Field	Definition
Server IP	IP address of the FTP server
Path and Filename	Path of a directory on the FTP server where you have write access for saving the backup copy of the configuration file. Specify a filename if you want to save the file under another name. For example, to save the configuration file in a file whose name identifies its origin and date (such as <code>KVM8802config040406</code>) in a directory called “upload” on the FTP server, you would enter the following in the “Path and Filename” field: <code>upload/KVM8802config040406</code> .
Username and Password	Username for accessing FTP server (check with the FTP server’s administrator, if needed to obtain the username and password to use),

▼ To Back Up or Retrieve KVM/net Configuration Data

1. In Expert mode, go to: Management > Backup Configuration.

The Backup Configuration form appears.

The screenshot shows the Cyclades management interface. The top navigation bar includes 'Access | Configuration | Information | Management'. The left sidebar lists various configuration options, with 'Backup Configuration' selected. The main content area displays the 'Backup Configuration' form. At the top right of the interface, there is a 'logout' link and system information: 'Host Name: ana-kom', 'IP Address: 192.168.45.21', and 'Model: KVM/net 16'. The form itself has a 'Type' dropdown menu set to 'FTP'. Below this are four input fields: 'Server IP', 'Path and Filename', 'Username', and 'Password'. At the bottom of the form are 'Save' and 'Load' buttons. The bottom of the interface features a 'Wizard' button and a row of control buttons: 'try changes', 'cancel changes', 'apply changes', 'reload page', 'Help', and 'no unsaved changes'.

2. To save or retrieve data from an FTP server, do the following:
 - a. From the Type drop-down list, select FTP.

A close-up of the 'Type' dropdown menu. The dropdown is open, and 'FTP' is selected and displayed in the text box to the left of the arrow.

Selecting FTP (default) brings up the fields displayed in the following figure.

A close-up of the Backup Configuration form fields. The 'Type' dropdown is set to 'FTP'. Below it are four input fields: 'Server IP', 'Path and Filename', 'Username', and 'Password'. At the bottom are 'Save' and 'Load' buttons.

Web Manager for Administrators

- b. Fill in the following fields with appropriate connection information:
 - Server IP
 - Path and Filename
 - Username
 - Password
3. Click Save to save the configuration to the selected location.
4. Click Load to load the configuration from the selected location.
5. Click “apply changes.”
6. To run the loaded configuration, reboot the KVM/net.

Firmware Upgrade

Selecting Management>Firmware Upgrade in Expert mode brings up the form shown in the following figure.

The screenshot shows a web interface for firmware upgrade. On the left is a sidebar menu with options: Backup Configuration, Firmware Upgrade (selected), Microcode Upgrade, Microcode Reset, KVM Port Sessions, and Reboot. The main area contains a warning box at the top. Below it are the following fields: Type (FTP), FTP Site, Username, Password, Path and Filename, and Run Checksum (No). An 'Upgrade Now' button is at the bottom.

You can use the form to set up automatic upgrades of the operating system and files on the KVM/net. The form collects information used to automatically download software from an FTP server and install the software on the KVM/net. The following table defines the information you need to supply on the form.

Field/Menu Name	Definition
Type	FTP is the only supported type.

Field/Menu Name	Definition
FTP Site	The address of the FTP server where the microcode is located. You can use any FTP server if you download the firmware on it first. The Cyclades FTP site address is: <code>ftp.cyclades.com</code> . If desired, see “To Upgrade Firmware [Expert]” on page 259 for how to download the firmware for installation on your own local FTP server.
Username	Username recognized by the FTP server. The Cyclades FTP username for microcode downloads is “anonymous.”
Password	Password associated with the Username. An empty password is accepted for anonymous login at the Cyclades FTP server
Path and File Name	<p>The pathname of the software on the FTP server.</p> <p>On the Cyclades FTP server, the directory is under <code>pub/cyclades/alterpath/KVMnet/released/version_number/filename</code>, where <code>version_number</code> is <code>V_N.N.N</code>, and <code>N.N.N</code> is the most recent version number, for example, <code>1.2.1</code>. The filename includes the version number in the following format: <code>zImage_ons_NNN.bin</code>. The pathname for this example would be:</p> <pre>pub/cyclades/alterpath/KVMnet/released/V_1.2.0/ zImage_ons_121.bin</pre> <p>Go to <code>ftp://ftp.cyclades.com/pub/cyclades/alterpath/KVMnet/released</code> in a browser, if needed, to verify the correct pathname and file names for the software (<code>zImage</code>) for the KVM/net.</p>

The following table has links to the related procedures.

To Find the Cyclades Pathname for Firmware or Microcode Upgrades	Page 258
To Upgrade Firmware [Expert]	Page 259
To Download Microcode From an FTP Server [Expert]	Page 261

▼ **To Find the Cyclades Pathname for Firmware or Microcode Upgrades**

1. To find the correct filename for the firmware or microcode updates at Cyclades, Corp., enter the following address in a browser:

`ftp://ftp.cyclades.com/pub/cyclades/alterpath/KVMnet/released`

2. In the `released` directory, go to the directory with the latest version number by clicking on the name of the directory.

For example, if the `released` directory contains directories named `V_1.1.0` and `V_1.2.0`, you would click on the `V_1.2.0` directory name. In the version directory, you would see several files like those shown in the following figure.

```
1.0.5.6-04.10.18.4bin
KVM_v104.bin
KVMterm_v104.bin
KVMUSBterm_v106.bin
zImage_ons_120.bin
zImage_ons_120.md5
```

3. If upgrading the KVM/net kernel, applications, and configuration files, take a note of the filename of the file whose name starts with `zImage` and has the `.bin` suffix and go to “To Upgrade Firmware [Expert]” on page 267.
4. If upgrading the microcode on a KVM PS2 terminator, take a note of the filename of the file whose name starts with `KVMterm` and has the `.bin` suffix and go to “To Download Microcode From an FTP Server [Expert]” on page 269.
5. If upgrading the microcode on a KVM USB terminator, take a note of the filename of the file whose name starts with `KVMUSBterm` and has the `.bin` suffix and go to “To Download Microcode From an FTP Server [Expert]” on page 269.
6. If upgrading the KVM switch microcode, take a note of the filename of the file whose name starts with `KVM_vXXX` and has the `.bin` suffix and go to “To Download Microcode From an FTP Server [Expert]” on page 269.

7. If upgrading the microcode on KVM/net IP modules take a note of the filename of the file whose name starts with a series of numbers separated by dots, for example, 1.0.5.6-04.10.18.4.bin, and go to “To Download Microcode From an FTP Server [Expert]” on page 269.

▼ **To Upgrade Firmware [Expert]**

1. In the Web Manager, go to Management >Firmware Upgrade in Expert mode.

The Firmware Update form appears.

2. Choose FTP from the Type menu.
3. Enter the name of the FTP server in the “FTP Site” field.
The Cyclades FTP site address is: `ftp.cyclades.com`.
4. Enter the username recognized by the FTP server in the “Username” field.
The Cyclades FTP username for firmware downloads is “anonymous.”
5. Enter the password associated with the username on the FTP server in the “Password” field.

The Cyclades FTP server accepts any password for “anonymous” login.

6. Enter the pathname of the file on the FTP server. in the “Path and Filename” field.

On the Cyclades FTP server, the directory is under `pub/cyclades/alterpath/KVMnet/released/version_number/`

See “To Find the Cyclades Pathname for Firmware or Microcode Upgrades” on page 266, if needed.

7. Press the “Upgrade Now” button.
8. Click “apply changes.”

Microcode Upgrade

Selecting Management>Microcode Upgrade in Expert mode bring sup the following form.

You can use the form to specify information used to automatically download microcode from an FTP server and install the microcode on various KVM/net components. You can specify either the Cyclades FTP server, `ftp://ftp.cyclades.com`, or a local FTP server where you have previously downloaded the microcode.

The following table shows the terms used on the form, the corresponding component names, and the filename formats uses for each type of microcode.

Target Name Used on Form	Filename Format	Component
KVM Terminator	KVMterm_vNNN.bin	KVM Terminator (PS2)
	KVMUSBterm_vNNN.bin	KVM Terminator (USB)
KVM Switch (internal)	KVM_vNNN.bin	KVM switch (internal)
KVM Video Compression Modules	N.N.N.N-NN.NN.NN.N.bin	IP modules

You need to enter the actual pathname components in the “Directory” and “File Name” fields. If needed, go to: “To Find the Cyclades Pathname for Firmware or Microcode Upgrades” on page 266.

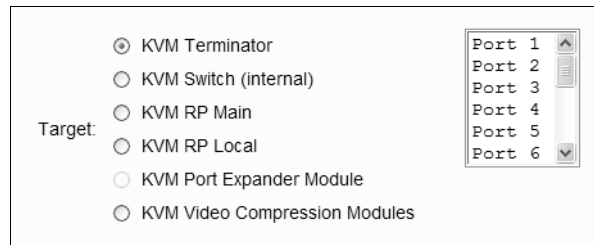
The following table defines the information you need to supply on the form.

Field Name	Definition
Target	The name of the component whose microcode you wish to upgrade.
FTP Server	The address of the FTP server where the microcode is located. You can use any FTP server if you download the firmware on it first. The Cyclades FTP site address is: <code>ftp.cyclades.com</code> .
Username	Username recognized by the FTP server. The Cyclades FTP username for microcode downloads is “anonymous.”
Password	Password associated with the Username. An empty password is accepted for anonymous login at the Cyclades FTP server
Directory	The pathname where the microcode resides on the FTP server. On the Cyclades FTP server, the directory is under <code>pub/cyclades/alterpath/KVMnet/released/version_number/filename</code> . Go to <code>ftp://ftp.cyclades.com/pub/cyclades/alterpath/KVMnet/released</code> in a browser, if needed, to verify the correct pathname and file names for the microcode for the KVM/net.
File Name	The file name of the microcode for the “Target.”

▼ **To Download Microcode From an FTP Server [Expert]**

1. Go to Management>Microcode Upgrade in Expert mode.
The Microcode form appears.
2. Click the radio button next to the “Target” whose microcode you want to update.
If you select the KVM Terminator radio button, a scrollable port list appears next to the Target list.

Web Manager for Administrators



The screenshot shows a web interface for selecting a target and a port. On the left, under the label "Target:", there are seven radio button options: "KVM Terminator" (which is selected), "KVM Switch (internal)", "KVM RP Main", "KVM RP Local", "KVM Port Expander Module", and "KVM Video Compression Modules". On the right, there is a scrollable list of ports labeled "Port 1" through "Port 6".

- 3.** To download microcode for a KVM Terminator, select a port from the scrollable port list.
- 4.** Enter the IP address or name of the FTP server in the “FTP Server” field.
The Cyclades FTP site address is: `ftp.cyclades.com`.
- 5.** Enter the username recognized by the FTP server in the “User” field.
The Cyclades FTP username for microcode downloads is “anonymous.”
- 6.** Enter the password associated with the username on the FTP server in the “Password” field.
The Cyclades FTP server accepts an empty password for “anonymous” login.
- 7.** Enter the pathname to the directory where the microcode resides on the FTP server. in the “Directory” field.
On the Cyclades FTP server, the directory is `pub/cyclades/alterpath/KVMnet/released/version_number/`
- 8.** Enter the name of the microcode file in the “File Name” field.
- 9.** Click the “Upgrade Now” button.
- 10.** Click “apply changes.”
- 11.** Go to “To Reset the Microcode After Upgrade [Expert]” on page 272.

Microcode Reset

Selecting Management>Microcode Reset in Expert mode brings up the form shown in the following figure.

You can use the form to reset the microcode after an upgrade.

▼ To Reset the Microcode After Upgrade

Perform this procedure if you have upgraded microcode as described in “To Upgrade Firmware [Expert]” on page 267.

1. From the top menu, select Management; from the side menu, select Microcode Reset.
The Microcode Reset form appears.
2. To reset the microcode in a KVM terminator, do the following steps.
 - a. Click the KVM Terminator radio button.
A scrollable list of KVM ports appears.
 - b. Select the port to which the KVM terminator is connected from the port list.
3. To reset another type of microcode, select the radio button next to the target you want to upgrade, either “KVM Switch (internal),” or “KVM Video Compression Modules.”
4. Press the “Reset Now” button.

Active Sessions

The Active Sessions form is designed to provide you quick status and usage information pertaining to all active server sessions. Administrators may also kill sessions from this form.

▼ To View Active Sessions Information

1. In Expert mode, go to Management>Active Sessions.

The Active Sessions window appears.



2. Review the session information as described in the following table.

Column	Definition
Uptime	Time the KVM/net has been on in minutes and seconds (mm:ss).
# Users	Number of users connected to server.
User	The user who initiated the session.

Column	Definition
TTY	The name of the KVM port.
From	The network machine to which the port is connected.
Login@	The day and time of the last login.
Idle	The time when the session or server became inactive.
JCPU	The duration of time used by all processes attached to the tty. It does not include past background jobs; only currently running background jobs.
PCPU	The time used by the current process that is named in the What column.
What	The current process attached to the tty.

3. Select the Refresh button to update the form with current information.

▼ **To Kill an Active Session**

1. In Expert mode, go to Management > Active Sessions.
The Active Sessions window appears.
2. Select the sessions you wish to kill.
3. Click Kill Session.
4. Click “apply changes.”

Reboot

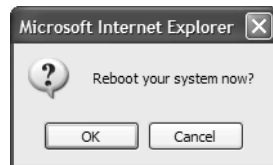
Selecting Management>Reboot in Expert mode, brings up the following form.



Selecting the Reboot button allows you to reboot the system without physically turning off the hardware.

▼ **To Reboot the KVM/net From a Remote Location**

1. In Expert mode, go to: Management>Reboot
2. Click the Reboot button.
3. A confirmation page appears.



4. Click OK to reboot the system.

Chapter 5

Web Manager for Regular Users

With the KVM/net Web Manager, regular users can connect to USB Sun servers running Solaris or PCs running a Windows, Linux, or other open source operating system through out-of-band, KVM connections and manage power of devices connected to AlterPath PMs from anywhere on a network. You can also connect to Windows Terminal Servers through in-band connections.

For more information on in-band and out-of-band connections see “Server Access: In-band and Out of Band” on page 36.

For more information on power management, see “Power Management for Regular Users” on page 273.

For procedures on how to operate the KVM/net as an administrator, see Chapter 4: Web Manager for Administrators.

Web Manager for Regular Users

When users without administrative privileges log in to the KVM/net, the Web Manager appears with three menu options:

- Connect to Server – Form used to connect to servers with either an in-band or a KVM connection.
See “Connecting to Servers Remotely Through the Web Manager” on page 286.
- Power Management – Form used to control the power of devices plugged in to AlterPath PM IPDUs.
See “Power Management for Regular Users” on page 273.
- Security – Form used to change your password.
See “Changing Your KVM/net Password” on page 274.

The Power Management and Security forms can be accessed by clicking the corresponding menu items.

The Web Manager interface provides you with a static main menu and a user entry form as displayed in Figure 5-1. The content of the user entry form changes based on your menu selection.

Web Manager for Regular Users

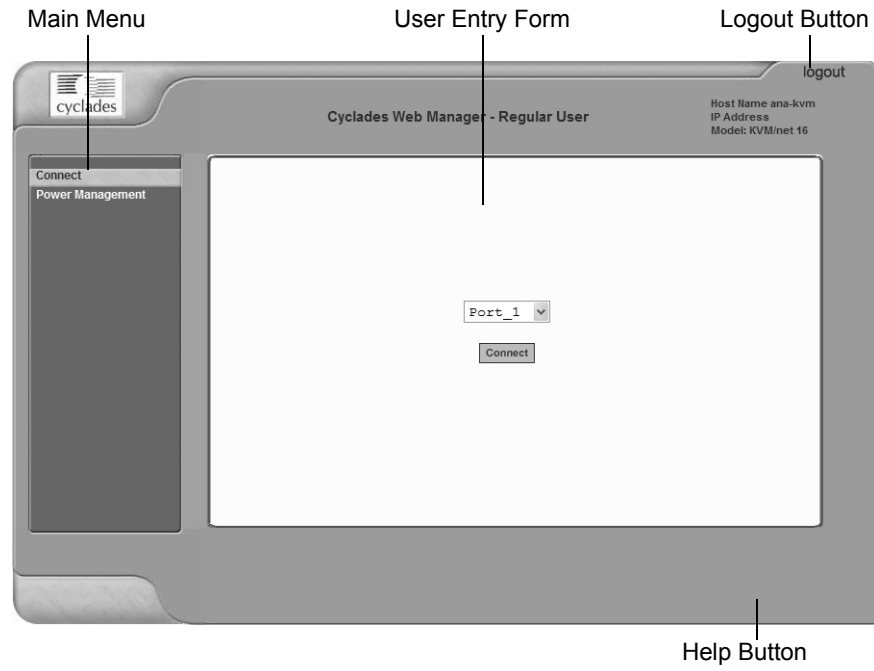


Figure 5-1: Cyclades KVM/net Web Manager

Prerequisites for Logging in to the Web Manager

You must collect the following information from your KVM/net administrator before accessing and logging into the KVM/net:

- KVM/net IP address
- Username
- Password

See the “Prerequisites for Accessing Servers With a KVM Connection” on page 131 for prerequisites for accessing servers.

See the following sections for prerequisites for accessing servers with KVM and in-band connections:

- “Prerequisites for Accessing Servers With In-band Connections” on page 280
- “Prerequisites for Accessing Servers With KVM Connections” on page 281

▼ ***To Log Into the KVM/net Web Manager as a Regular User***

1. Launch a supported browser and type the KVM/net IP address (for example `http://10.0.0.1/`) into the browser’s URL field.

The AlterPath KVM/net log in screen appears.

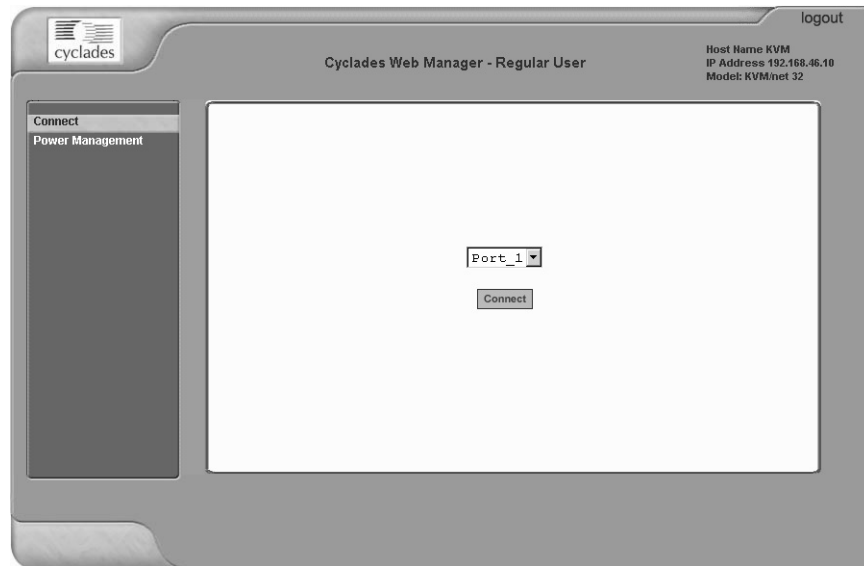
Prerequisites for Logging in to the Web Manager



2. Enter your username and password as provided to you by your KVM/net administrator

3. Click Go.

The Connect form appears.



Web Manager for Regular Users

See “Web Manager for Regular Users” on page 268 for an introduction to using the Web Manager and links to more detailed information.

Power Management for Regular Users

The KVM/net offers two modes of controlling power:

- Power control of any device plugged into a PM that is configured on the KVM/net.

See “Power Control of Any Device Plugged Into a PM on the KVM/net” on page 273.

- Power control of a server while connected to that server through a KVM port.

See “Controlling Power of a KVM-connected Server” on page 301.

Power Control of Any Device Plugged Into a PM on the KVM/net

Depending on your access rights, the KVM/net allows you to remotely view and manage all PMs connected to the KVM/net. Regular users can go to the IPDUs Power Management menu on the Web Manager and use the Outlets Manager and the View IPDUs Info forms to manage and view the status of PMs and the devices plugged into them. The following table lists the power management tasks available to regular users through the Web Manager and links to the associated procedures.

Table 5-1: Power Management Tasks Available to Regular Users

Task	Where Documented
Switch on/off and lock/unlock outlets; reboot network devices.	<ul style="list-style-type: none"> • “Outlets Manager” on page 145 • “To View Status, Lock, Unlock, and Cycle Power Outlets [Expert]” on page 146
View IPDU information by ports and slaves.	<ul style="list-style-type: none"> • “View IPDUs Info” on page 147 • “To View and Reset IPDU Information [Expert]” on page 147
Switch on/off and lock/unlock outlets; reboot servers connected to KVM ports.	<ul style="list-style-type: none"> • “To Power On, Power Off, or Reboot the Connected Server [KVM]” on page 320

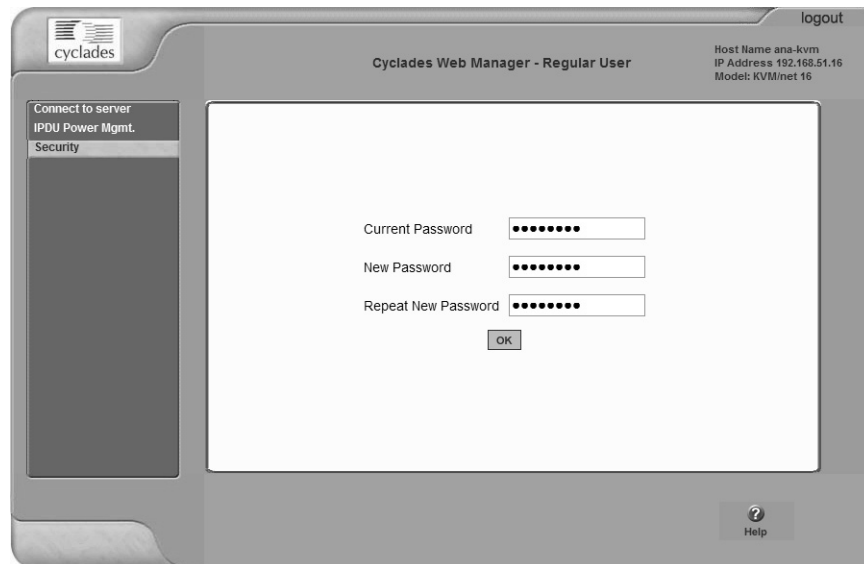
Changing Your KVM/net Password

On the Security form on the KVM/net Web Manager, you can change your old password to a new password.

▼ *To Change Your KVM/net Password*

1. Log in to the Web Manager.
2. Select Security in the Main Menu.

The Security Form appears.



The screenshot shows the Cyclades Web Manager interface for a regular user. The page title is "Cyclades Web Manager - Regular User". In the top right corner, there is a "logout" link and system information: "Host Name ana-kvm", "IP Address 192.168.51.16", and "Model: KVM/net 16". On the left side, there is a navigation menu with options: "Connect to server", "IPDU Power Mgmt.", and "Security". The "Security" option is selected. The main content area contains three password input fields: "Current Password", "New Password", and "Repeat New Password". Each field is filled with ten black dots. Below the "Repeat New Password" field is an "OK" button. In the bottom right corner of the interface, there is a "Help" button with a question mark icon.

3. Type your current password in the Current Password field.
4. Type your new password in the New Password field and again in the Repeat New Password field.
5. Click OK.

Chapter 6

Accessing Connected Devices

With the KVM/net, users and administrators can connect to any PC or USB Sun servers through out-of-band, KVM connections and manage power of devices connected to AlterPath PMs from anywhere on a network with the Web Manager or locally with the OSD. Users and administrators can also connect to Windows Terminal Servers through in-band connections. .

This chapter gives an overview of the options for accessing servers that are connected to ports on the KVM/net.

The following table lists the procedures in this chapter.

To Connect to a KVM Port Through the Login Screen	Page 288
To Connect to Servers Through The Web Manager's Connect To Server Form	Page 290
To Connect to Servers Through the OSD Connection Menu	Page 293
To Return to the Connection Menu After Connecting to a Port	Page 297
To View Connected Port Information	Page 297
To Initiate Cycle by Server	Page 298
To Connect to the Next Authorized Server from the Current Server	Page 299
To Connect to the Previous Authorized Server from the Current Server	Page 299
To Adjust Screen Brightness and Contrast	Page 299
To Reset the Keyboard and Mouse	Page 300
To Power On, Power Off, or Reboot the Connected Server	Page 301
To Close a KVM Connection	Page 302
To Power On, Power Off, Lock, Unlock, or Cycle Devices Plugged into PM Outlets	Page 310
To Configure a PPP Connection on a Remote Computer	Page 313

Who Can Access Connected Devices

Authorized users have the permissions they need to access one or more servers or other devices that are connected to ports on the KVM/net. See “Types of Users” on page 16 and “KVM/net Port Permissions” on page 26 for more information.

Authorized users and KVM/net administrators have the following options for accessing the connected devices:

- Use the Web Manager for most connections to devices.
See “Cyclades Web Manager” on page 21 and “Prerequisites for Using the Web Manager” on page 22 for background information about the Web Manager, if needed.
Chapter 4: “Web Manager for Administrators” describes how KVM/net administrators can access connected devices through the Web Manager.
Chapter 5: “Web Manager for Regular Users” describes how authorized users can access connected devices through the Web Manager.
See “Connecting to Servers Remotely Through the Web Manager” on page 286 and “Controlling KVM Port Connections” on page 294 for instructions on how to log into the Web Manager and connect to devices.

- Use the on-screen display (OSD) to access devices that are connected to the KVM/net's KVM ports.

Local users and administrators who have access to a directly-connected Local User station can use the OSD Connect menu.

Chapter 7: "On Screen Display" describes how to access connected devices through the OSD.

- Dial into the KVM/net through a modem
See "Modem Connections" on page 312.

Server Connections: What You See

Once connected to a server, one or two windows appear depending on the type of server connection being made:

- KVM connections
 - AlterPath Viewer is launched with the same interface as if you were directly logging into the connected server.
 - The Access Window with an interface for managing up to four server connections.

See "Viewing KVM Connections" on page 278.

- In-band connections

An ActiveX viewer is launched with the same interface as if you were directly logging into the connected server.

See "Viewing In-band Connections" on page 280.

Viewing KVM Connections

The AlterPath Viewer is the interface you use to manage servers over KVM over IP connections. Logins persist across connection sessions. If you close a connection without logging out, you are still logged in the next time you connect, unless the system has closed your session. If you are not currently logged in, you see a login screen or prompt.

The connected servers's login prompt appears. The following example shows a login prompt for a Windows 2000 server displayed by the AlterPath Viewer. If you are connected to a Linux server without a graphical display, you see a "Login:" prompt.



Figure 6-1: AlterPath Viewer for KVM Connections

Server Connections: What You See

See “AlterPath Viewer Settings” on page 305 for more detailed information about using the AlterPath Viewer.

Local KVM connections through the OSD do not use the AlterPath Viewer. Instead, the view of the connected server takes up the entire screen of local work station. See “Controlling KVM Port Connections” on page 294 for more information local KVM connections.

Viewing In-band Connections

The ActiveX viewer is the interface you use to manage servers over an in-band connection.

The following graphic displays the login screen of a server running Windows 2003 in the ActiveX viewer for in-band connections.



Figure 6-2: ActiveX Viewer for In-band Connections

Prerequisites for Accessing Servers With In-band Connections

A KVM/net user who needs to access any RDP server must have the following:

- The username and password of a valid account on the RDP server.
- Internet access and Microsoft Internet Explorer on a remote Windows client machine.

Prerequisites for Accessing Servers With KVM Connections

The following prerequisites must be met before you can access a KVM-connected server:

- Know the KVM Port(s) to which you have access (especially if direct access to a port is configured)
- Have the username and password of a valid account on the connected server
- If you are connecting through the Web Manager, have the following:
 - A remote computer running a Windows operating system with Internet access and a supported browser installed
 - The IP address of the KVM/net
- If you are making a local connection, have a direct connection made to the User 1 or User 2 ports of the KVM

Web Manager Login Screen

The following table lists the sections that describe the three different possible views of the Web Manager login screen that can appear under various conditions.

Table 6-1: Web Manager Login Screen Options

Conditions	Where Documented
Direct logins to KVM ports not enabled: <ul style="list-style-type: none"> • You enter the KVM/net's IP address in a browser to bring up the Web Manager login screen. • You can log into the Web Manager and perform administration. • If you want to access a server connected to a KVM port after logging into the Web Manager, you can connect to the KVM port from the Connect to Server form. 	"Login Screen: Direct Logins Not Enabled" on page 104

Table 6-1: Web Manager Login Screen Options (Continued)

Conditions	Where Documented
<p>Direct logins to KVM ports enabled (option 1):</p> <ul style="list-style-type: none"> • You enter the KVM/net’s IP address in a browser to bring up the Web Manager login screen. • You enter your username and password and the desired KVM port number on the Web Manager login screen and connect to a KVM port directly without logging into the Web Manager first. 	<p>“Login Screen: Direct Logins Enabled, Only IP Address Entered” on page 105</p>
<p>Direct logins to KVM ports enabled (option 2):</p> <ul style="list-style-type: none"> • You enter the KVM/net’s IP address along with the port name in a browser to bring up the Web Manager login screen. • The port field is already filled in when the Web Manager appears. • You save the URL that includes the port in a favorites file to save time when logging into the same port in the future. • You enter your username and password on the Web Manager login screen and connect to a KVM port directly without logging into the Web Manager first, as in the previous row. 	<p>“Login Screen: Direct Logins Enabled, IP Address and Port Entered” on page 106</p>

Login Screen: Direct Logins Not Enabled

The following screen shows an example of the Web Manager login screen as it appears if the following two conditions are true:

- The IP address of the KVM/net is entered in the browser.
- Direct logins to KVM ports is not enabled.



Figure 6-3: Web Manager Login Screen Without KVM Direct Logins Enabled

As shown in Figure 3-1, the Web Manager login screen displays two fields in the “Login” section: “username” and “password.” The product name appears in the “Welcome” line, and the model and the administrator-specified hostname are listed below images of the front and back of the product.

Login Screen: Direct Logins Enabled, Only IP Address Entered

The following screen shows an example of the format of the Login portion of the Web Manager login screen as it appears if the following two conditions are true:

- The IP address of the KVM/net is entered in a browser
- Direct logins to KVM ports is enabled.



The screenshot shows a login form with the following fields and values:

- username: ana
- password: [masked with three dots]
- port: 2

A "GO" button is located at the bottom right of the form.

Login Screen: Direct Logins Enabled, IP Address and Port Entered

This section describes how the Web Manager login screen appears if the following two conditions are true:

- Direct logins to KVM ports is enabled,
- The IP address of the KVM/net is entered along with a port ID (in the required format) in a browser

The required format is:

```
IP_address/login.asp?portname=portnumber
```

where *IP_address* is the IP address of the KVM/net and *portnumber* is the portnumber or alias assigned to the KVM port.

Web Manager Login Screen

Entering the port number along with the IP address makes it possible to connect directly to a KVM port without going to the Web Manager's Access page first. You can save the URL as a bookmark or in your browser's favorites list and go directly to the port login later without typing in the entire URL. The "port" field is filled in with the port number when the Web Manager login window appears.

The example in the following figure shows `http://192.168.46.169/login.asp?portname=Port_1` entered in the Address field of a Microsoft Internet Explorer browser. The login screen displays empty "username" and "password" fields and a port field filled with the name of the port from the URL, in this case "Port_1."



Connecting to Servers Remotely Through the Web Manager

KVM/net administrators who are logging into the Web Manager to perform KVM/net configuration can use any modern browser (such as Internet Explorer 5.5 or above, Netscape 6.0 or above, Mozilla or Firefox).

Authorized users can connect to servers in the following ways:

- By accessing the Web Manager through a browser, logging into the Web Manager, and then connecting to the device from the Connect form.
This method applies to both KVM and in-band connections. If direct access to KVM ports is not enabled, the authorized user first brings up the Web Manager in a supported browser, logs into the Web Manager, and then connects to the device.
See “To Connect to Servers Through The Web Manager’s Connect To Server Form” on page 290 for instructions on using this method.
- If direct access to KVM ports is enabled, the authorized user can connect directly to a KVM port by one of the two following methods:
 - Bringing up the Web Manager by entering the IP address of the KVM/net in a browser and then entering the port number on the login screen.
See “Login Screen: Direct Logins Enabled, Only IP Address Entered” on page 284 for more details.
 - Bringing up the Web Manager with the port number already entered in the “port” field, by including the port name along with the IP address (in the required format) in the browser.
See “Login Screen: Direct Logins Enabled, IP Address and Port Entered” on page 284 for more details.

Note: The direct access method allows users to access servers that are connected to KVM ports only or servers that are connected to KVM ports and are available for in-band access as well. This method is particularly useful for users who may need direct KVM access to a server that has both KVM and in-band access enabled.

The KVM connections brings up the AlterPath Viewer with a login prompt for the connected server, and the in-band connections brings up an ActiveX viewer. Any of these connection options also brings up the Access Window

displaying the status of and management options for up to four server connections. See “Server Connections: What You See” on page 277 for a description of the AlterPath Viewer and the Access Window.

Identifying Servers and their Connection Type in the Connect to Server Drop-down List

There are two levels of identifying servers in the Connect to Server drop-down list:

- **Connection Type** – The types of connections that can be made to each server is displayed in parenthesis at the end of each server entry in the list. An entry with “(KVM)” at the end of it can be accessed with a KVM connection only. An entry with “(Inband)” at the end of it can be accessed with an in-band connection only. An entry with “(KVM + Inband)” can be accessed with both connection methods. See “Determining the Connection Type and its Supported Functionality” on page 33 for more detailed information.
- **Server Name or Port Name/Number** – The type of connection determines the type of name applied:
 - Individual KVM ports are either labelled by the port number in the form Port_# or by an administrator-defined alias, which should describe the type of computer connected to the port or be the actual name of the connected server.
 - Individual in-band connections are labelled by an administrator-defined server name, which should identify the type of computer being accessed or be the actual name of the server.

Note: A server that is configured for both in-band and KVM connections can have two different aliases configured: one for the KVM port and one for the in-band connection. In this case, the alias that appears in the Connect to Server drop-down list is the alias assigned to the KVM port.

Reading the Port Numbers of Cascaded KVM Devices

In the Connect drop-down list on the Connect to Server form, a name and a number connected by a period (.) indicate the alias or name of the cascaded KVM unit followed by its physical port.

For example, in the port name kvm2.4, kvm2 is the name of the cascaded device, and 4 is the physical port on the device named kvm2.

The following table lists the login procedures for all types of user.

To Log Into the KVM/net Web Manager as a Regular User as Admin	Page 270
To Log Into the Web Manager as Admin as a Regular User	Page 128
To Connect to a KVM Port Through the Login Screen	Page 288
To Connect to Servers Through The Web Manager's Connect To Server Form	Page 290

▼ To Connect to a KVM Port Through the Login Screen

This procedure assumes that the KVM/net administrator has enabled direct logins to KVM ports.

1. Enter the IP address of the KVM/net alone or the IP address of the KVM/net followed by the KVM port number (in the required format) in the address field of a browser.

The required format for entering a KVM port number in the URL is:

```
IP_address/login.asp?portname=portnumber
```

where *IP_address* is the IP address of the KVM/net and *portnumber* is the portnumber or alias assigned to the KVM port.

Note: Check with the administrator who configured the basic network parameters on the KVM/net, for help finding the IP address and the “admin” password, if needed. Also if needed, see an example of the proper format for entering the port number in “Login Screen: Direct Logins Enabled, IP Address and Port Entered” on page 106.

- If DHCP is not enabled, use a fixed IP address assigned by the network administrator to the KVM/net.
- If DHCP is enabled, enter the dynamically-assigned IP address.

The Web Manager login screen appears. If you entered a KVM port ID in the URL, the “port field” is filled in with the port ID you entered.

2. If you entered a KVM port ID in the URL, save the URL as a bookmark or in your favorites list in the browser.

For future connections to that port, you can click on the bookmark or item in favorites list to easily bring up the Web Manager login screen again with the port number filled in.

3. Enter your account name in “username” field and the account’s password in the “password” field.
4. If no port is listed in the “port” field, enter a port alias or number.
5. Press “Go.”

If the Web Manager Access “Connect to Server” form appears, you are finished logging in.

6. For administrators, if a dialog box prompts you to verify whether you want to proceed by logging the other admin out or by cancelling your login attempt, click the appropriate radio button and then click Apply.

Note: Only one admin can be logged in at a time.

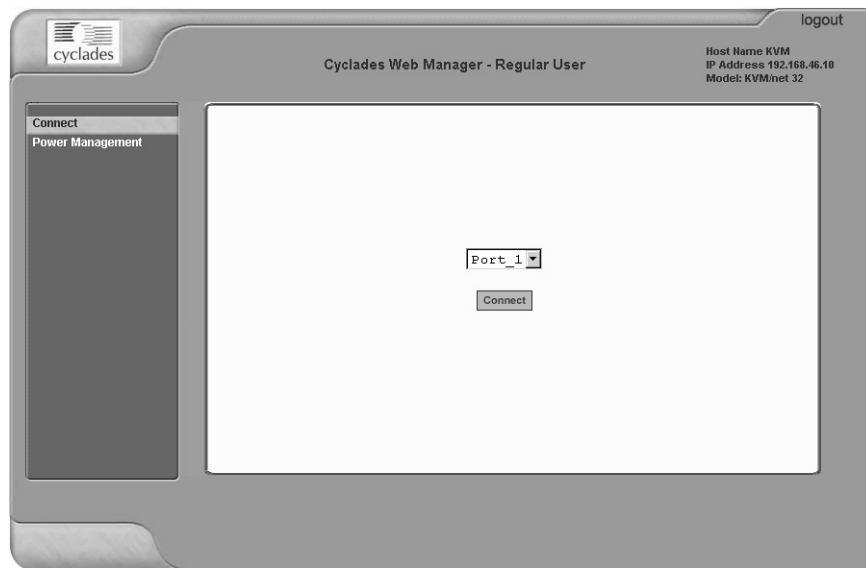
▼ **To Connect to Servers Through The Web Manager's Connect To Server Form**

1. Log in to the KVM/net using your username and password.

See “To Log Into the KVM/net Web Manager as a Regular User” on page 270 or “To Log Into the Web Manager as Admin” on page 128 for detailed instructions on logging in to the Web Manager.

2. From the left menu panel, select Connect to Server.

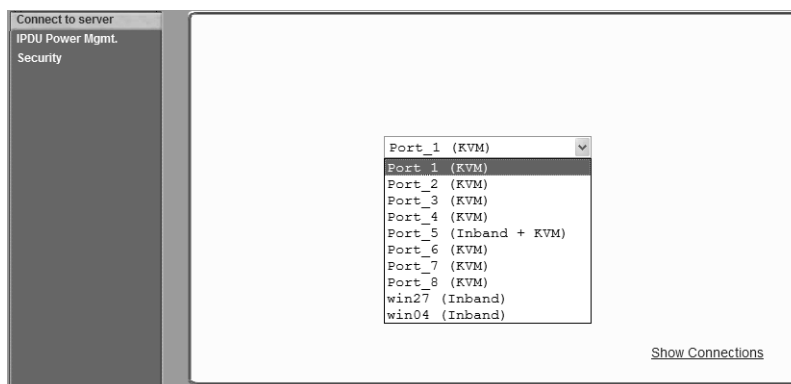
The Port Connection form appears.



3. From the drop-down menu, select the server or port to which you want to connect.

A list similar to the list in the following graphic appears.

Connecting to Servers Remotely Through the Web Manager



See “Determining the Connection Type and its Supported Functionality” on page 33 for a description of each type of connection method and what happens once connected.

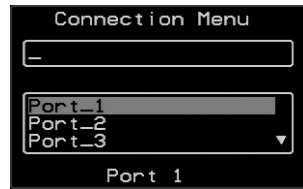
4. Click on the Connect button.

The system may launch one or two browser windows: the AlterPath viewer and the Access Window for KVM connections, or an ActiveX viewer for RDP connections. See “Server Connections: What You See” on page 277 for a description of each window.

Note: The first time the system invokes the AlterPath Viewer, it prompts you to accept a security certificate. Click Accept.

Connecting to Servers Locally Through the OSD

Administrators and authorized regular users who have local access to the KVM/net can use the Connection Menu, as displayed in the following figure, to connect to and control servers that are connected to KVM ports on the master KVM/net or on any cascaded KVM device.



Access to the OSD requires a local keyboard, monitor, and mouse connected to the KVM management ports, User 1 or User 2, on the back of the KVM/net. See “To Connect to the User 1 Management Port” on page 75 for instructions on connecting to the User 1 port, or see “To Connect the RP to the KVM/net” on page 120 for instructions on connecting to the User 2 port.

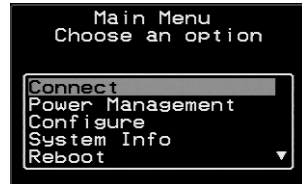
Connections made through the OSD are to physically connected devices only. Use the Web Manager to connect to a remote device. See “To Connect to Servers Through The Web Manager’s Connect To Server Form” on page 290 for instructions.

Note: The OSD cannot be used to access in-band servers. See “Connecting to Servers Remotely Through the Web Manager” on page 286 for information and instructions on accessing in-band servers.

▼ To Connect to Servers Through the OSD Connection Menu

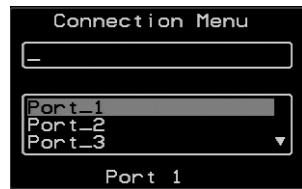
1. On the OSD Login window, enter your username and password as provided to you by the KVM/net administrator.

The OSD Main Menu appears.



2. From the OSD Main Menu, select Connect.

The Connection Menu appears.



3. To select the port you wish to connect to, do one of the following procedures:
 - Type the first letters of the port name in the quick search box until the desired port is highlighted in the port list box.
This field is case-sensitive.
 - Select the desired port using the port list box.
4. Press Enter.

Your monitor displays the work station of the connected server.

See Table 6-2, “Tasks Available While Connected to KVM Ports,” on page 294 for a complete lists of the tasks available while connected to KVM ports and references to the related instructions.

Controlling KVM Port Connections

Once connected to a server, you may want to do one or more of the procedures listed in the following table.

Table 6-2: Tasks Available While Connected to KVM Ports

Task	Where Documented
Return to the OSD Connection menu after connecting to a port.	“To Return to the Connection Menu After Connecting to a Port” on page 297.
Access a port that is already in use by another user.	“Sharing KVM Port Connections” on page 303
Make direct connections to other servers without returning to the OSD Connection Menu.	<ul style="list-style-type: none"> • “To Initiate Cycle by Server” on page 298 • “To Connect to the Next Authorized Server from the Current Server” on page 299 • “To Connect to the Previous Authorized Server from the Current Server” on page 299
Reset your keyboard and mouse.	“To Reset the Keyboard and Mouse” on page 300
Adjust the color and brightness of the server window.	“To Adjust Screen Brightness and Contrast” on page 299
Power on, power off, or reboot the connected server.	“To Power On, Power Off, or Reboot the Connected Server” on page 301
View information about the currently selected port.	“To View Connected Port Information” on page 297

Hot Keys for KVM Connections

Predefined keyboard shortcuts (also called hot keys) allow you to perform common actions and launch management windows while connected through a KVM port.

The default hot keys are described in the following table. A plus (+) between two keys indicates that both keys must be pressed at once. When two keys are separated by a space, each key must be pressed separately. For example, “Ctrl+k p” means to press the Ctrl and “k” keys together followed by the “p” key, and “Ctrl Shift+i” means press the Ctrl key followed by the Shift and “i” keys pressed together.

Table 6-3: Default KVM Connection Keyboard Shortcuts

Key Combination	Action
Ctrl+k q	Quit. Closes the connection to the current KVM port and ends the KVM connection.
Ctrl+k p	Power management. Brings a power management menu with the options to turn on, off, or cycle the power for outlets to which the current server is connected.
Ctrl+k .	Next Port. Goes to the next authorized port.
Ctrl+k ,	Previous Port. Returns to the previous authorized port.
Ctrl+k v	Video. Brings up a menu that allows you to change between “Automatic control” (which compensates for the length of the cable running from the KVM/net to the KVM terminator that is connected to the server) and “Manual control” for adjusting screen brightness and contrast.
Ctrl+k s	Reset keyboard and mouse. Allows you to reset the keyboard and mouse if either of them stops responding.

The KVM/net administrator may redefine the keyboard shortcuts, as described in “Redefining KVM Connection Hot Keys” on page 37. If the defaults shown in the previous table do not work, check with your KVM/net administrator for the site-specified keys to use.

Hot Keys for Emulating Sun Keyboard Keys

The KVM/net provides a default set of hot keys for use while connected to Sun servers. You can use the Sun hot keys to emulate keys that are present on Sun keyboards but are not present on Windows keyboards.

The hot keys are made up of an escape key followed by a function key. The default escape key is the Windows key, which is labeled with the Windows logo. The Windows key usually appears on the Windows keyboard between the `Ctrl` and `Alt` keys. The following table shows function keys and keys from the numeric keypad that emulate Sun equivalent keys when you enter them at the same time as the hot key. For example, to use the Sun `Find` key, you would press the Windows key at the same time you press the `F9` function key.

Table 6-4: Default Sun Key Emulation Hot Keys

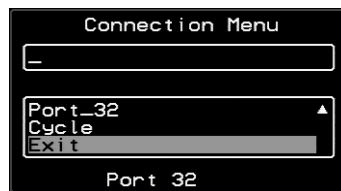
	Win Key	Sun Key
Function Keys	F2	Again
	F3	Props
	F4	Undo
	F5	Front
	F6	Copy
	F7	Open
	F8	Paste
	F9	Find
	F10	Cut
	F11	Help
	F12	Mute
	Numeric Keypad Keys	*
+		Vol +
-		Vol -

KVM/net administrators can change the default escape key portion of the Sun keyboard emulation hot keys from the Windows key to any of the following: Ctrl, Shift, or Alt. See “Redefining Sun Keyboard Equivalent Hot Keys” on page 37 for details and links to procedures.

▼ **To Return to the Connection Menu After Connecting to a Port**

1. Press Ctrl+k q to display the OSD Connect Menu.

The Connection Menu appears.



2. Do one of the following:

- To make a new server connection, select another port from the list.
- To return to the Main Menu, select Exit.
- To cycle through all servers, select Cycle.

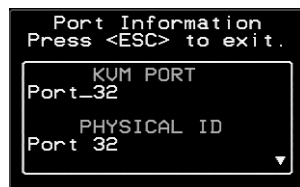
The cycle option does not appear when you are connected through the Web Manager.

▼ **To View Connected Port Information**

1. Use the information keyboard shortcut.

The default is **Ctrl+k i**.

The following window appears.



2. Press Esc to exit the Port Information window and return to the connected server.

Cycling Between Servers

Cycle refers to the capability to connect to one or more authorized servers from the server to which you are currently connected. Through the OSD menus or by using a keyboard shortcut, you have immediate access to all configured and authorized servers.

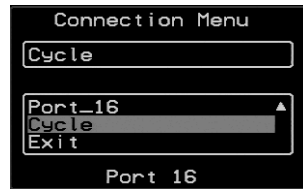
There are two types of cycle commands:

- Cycle by Server – View all authorized servers on a continuous basis until all servers have been exhausted and then start over again.
- Cycle by Key Sequence – View or access the server connected to the next or previous port in the Connection Menu list.

The servers are cycled in the order in which their ports are listed in the Server Connection form.

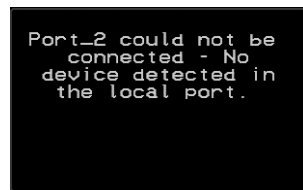
▼ To Initiate Cycle by Server

1. From the Connection Menu, choose Cycle.



2. Select Cycle at the bottom of the list.

The system initiates the cycle from the first authorized server, and the servers connected to all authorized ports appear for a few moments. If there is no device attached to the port associated with the next logical port, a message appears to indicate that there is no device connected.



3. To abort the process and close the session, press the escape sequence.

The default is Ctrl+k q.

▼ **To Connect to the Next Authorized Server from the Current Server**

- Use the Next keyboard shortcut.
The default is **Ctrl+k .**
The next authorized server appears. Repeat this step to move to the next server.

▼ **To Connect to the Previous Authorized Server from the Current Server**

- Use the Previous keyboard shortcut.
The default is **Ctrl+k ,**
The previous authorized server appears. Repeat this step to move to the previous server.

▼ **To Adjust Screen Brightness and Contrast**

1. Press the video control keyboard shortcut.

The default is **Ctrl+k v**.

Depending on which window was accessed last, one of the following windows appears.

- Automatic Control



- Manual Control



Accessing Connected Devices

2. To switch to the Auto control window or the Manual control window select Auto or Manual respectively.
3. To adjust screen brightness and contrast on the Automatic Control window, select the right or left arrows to set the desired adjustment value.

The Automatic Control window is used to compensate for cable length. For example, if you use a 500-foot cable, the setting might be 10 or 20. If a shorter cable such as 6 or 3 feet is used, a value of 128 or 150 is more appropriate. If this setting is not adjusted properly, the video quality may be poor.

4. To adjust screen brightness and contrast on the Manual control page, select the arrow keys to increase or decrease the contrast and brightness.

The Manual Control window is used to control the levels of video brightness and contrast. The higher the value, the greater the brightness and contrast will be.

Resetting the Keyboard and Mouse

You can use the “Keyboard/Mouse Reset” hot key to bring up the “Reset keyboard and mouse?” screen if the keyboard and mouse is not working properly when accessing a server through a KVM port. This command is equivalent to unplugging and plugging in again the keyboard and mouse.

▼ *To Reset the Keyboard and Mouse*

1. Type the “Keyboard/Mouse Reset” hot key.

The default is Ctrl-k s. The following confirmation window appears.



2. Select Yes to enable your keyboard and mouse again.

Note: See also the “Avoiding Conflicting Mouse Settings” on page 96.

Controlling Power of a KVM-connected Server

In order to control power of a server while connected to the server, the following conditions must be met:

- The server must have at least one power cord plugged into an AlterPath PM that is properly configured and connected to the AUX port.
- The power outlet(s) that the server is connected to must be configured to the port.
- If a regular user is accessing this device, the user must have the following permissions:
 - Full control (read, write, power) permission on the port,
 - Permission to control power on the PM outlet that the device is plugged into.

▼ To Power On, Power Off, or Reboot the Connected Server

1. While connected to a server, use the power management keyboard shortcut.

The default is **Ctrl+k p**.

A window similar to the following appears.



2. Select the configured outlet.
3. Do one of the following:
 - To turn the power on, select On.
 - To turn the power off, select Off.
 - To reboot, select Cycle.

To lock or unlock outlets, you must go to the Power Management menu. See "Power Management" on page 309 for more information.

Closing a KVM Connection

The ways you can close a KVM connection are listed below:

- For IP connections, select “Exit Viewer Client” from the AlterPath Viewer Shortcuts menu.
- Use a hot key sequence (Ctrl+k q) to bring up the Connection menu, then select the Exit option.
- Let the session time out.

▼ *To Close a KVM Connection*

Do one of the following steps.

- 1.** To use the menu option from the AlterPath Viewer menu bar, go to Shortcuts and select “Exit Viewer Client.”

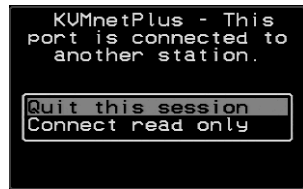
- OR -

- 2.** To use the escape hot key, do the following steps.
 - a. Type the hot key escape sequence.
Ctrl+k q is the default.
The Connection menu appears.
 - b. Type “e” in the text field to highlight the Exit option.
 - c. Click Enter.

Sharing KVM Port Connections

Two authorized users can connect simultaneously to a single KVM port.

When a user connects to a KVM port that is already in use, the software presents a menu to the connecting user. The options on the menu depend on the connecting user's access permissions. The following figure shows two options that are always presented on the menu to the connecting user.

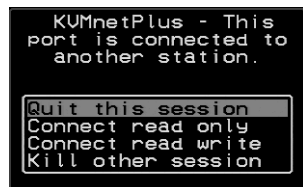


The two menu options are described in the following table.

Quit this session	Ends the connection attempt and returns the user to the Connection Menu
Connect read only	Connects the user in read-only mode and sends this notice to the current user:



If the connecting user has either read-write, or full access permissions for the KVM port, additional menu options appear, as shown in the following figure.



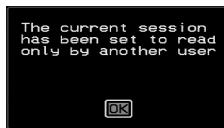
Accessing Connected Devices

The two menu options are described in the following table.

Connect read write	Connects the new user in read-write mode and sends this notice to the current user.
---------------------------	---



If the previous user is in read-write mode, that user's mode is changed to read-only and the user sees the following notice:



Kill other session	Kills the existing session and connects the new user in read-write mode. Sends the following notice to the current user and disconnects that user:
---------------------------	--



When the current user is in read only mode, the connecting user is always granted the highest level of access for which the connecting user is authorized.

If two users are connected to a KVM port, either user may choose at any time to change the access mode or disconnect from the session by issuing a hot key or Esc.

AlterPath Viewer Settings

You can configure the AlterPath viewer settings from the top menu.

Shortcuts Options Connection Host OS About...

For a definition of the menu settings, refer to the tables below. A T1 connection is recommended for best performance when using the AlterPath Viewer.

Recommended Settings

The recommended AlterPath Viewer settings are listed in the following table. The connection you set must reflect your actual Internet connection method.

Menu	Select the following option(s):
Options	Auto Sync Mouse
Connection	T1 (preferred), No Encryption, High Color
Host OS	Auto/Other

Options Menu

The following table describes the items in the AlterPath Viewer's Options menu, which you can change as needed for your own requirements.

Menu Selection	Description
Force Screen Refresh	Refreshes the viewer.
Force Screen Auto Alignment	Switches to Auto Alignment mode, which may change the position of the viewer. (You can manually configure Screen Alignment by going to Options>Viewer Options>Screen Alignment.)
Toggle Full Screen	Switches the viewer's display from window to full-screen mode or from full-screen to window mode.
Viewer Options	See Setting the Viewer Options
Show Frames/sec and Network bits/sec	Specify as needed.
Auto Sync Mouse	Make sure this is selected for KVM/net compatibility
Show Startup Dialog	Causes a menu to appear when the viewer is launched.

Setting the Viewer Options

The Viewer Options window allows you to align or position the viewer window and to fine tune the image. The configuration for these settings may vary from one system to another.

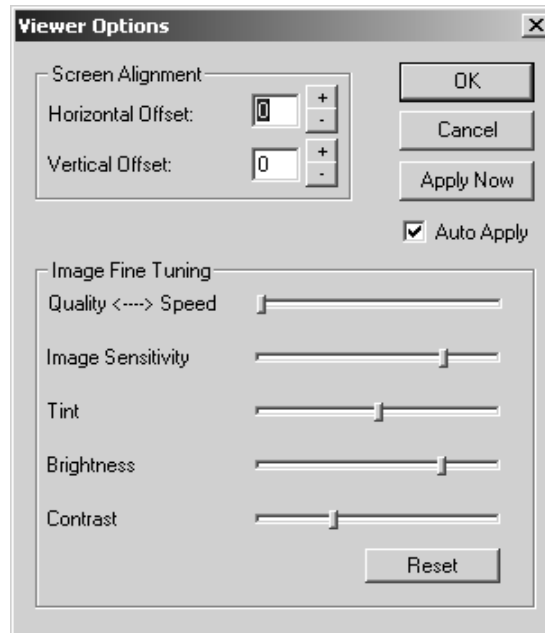


Figure 6-4: AlterPath Viewer Options Screen

The following table defines the fields and menu items.

Table 6-5: AlterPath Viewer>Options>Viewer Options Menu

Field or Menu Item	Function
Horizontal Offset	The horizontal coordinate for positioning the AlterPath Viewer on the screen (default = 0).
Vertical Offset	The vertical coordinate for positioning the AlterPath viewer on the screen (default = 0).
Quality <---->Speed	Move slider to the left to increase image quality; move slider to the right to increase the performance of the viewer.

Table 6-5: AlterPath Viewer>Options>Viewer Options Menu (Continued)

Field or Menu Item	Function
Image Sensitivity	Move slider to the right to increase the image sensitivity.
Tint	Move the slider in either direction to achieve the desired color. For a neutral (white) color, keep the slider in the middle.
Brightness	Move the slider to the right to increase screen brightness.
Contrast	Move the slider to the right to increase screen contrast.

Connection Menu

The following table describes the Connection menu options.

Menu Selection	Function
56K	For when your network connection method is a 56K modem
DSL	For when your network connection method is a DSL line
T1	Recommended connection type. For when your network connection method is a dedicated T1 line
Low BW LAN	For when you are connecting through a low bandwidth local area network
LAN	For when you are connecting through a standard speed local area network.
Auto	For setting the connection mode automatically
Encrypt Everything	For encrypting everything
Encrypt Keyboard and Mouse	For encrypting only keyboard and mouse input
Encryption Type	For either RC4 or Triple DES encryption

Menu Selection	Function
No Encryption	For no encryption
High Color	For high color resolution screens
Low Color	For low color resolution screens
Grey Scale	For grey scale screens
Low Grey Scale	For low resolution grey scale screens

Power Management

Administrators and authorized users can access Power Management windows, which allow you to check the status of the master IPDU connected to the AUX port in addition to all cascaded IPDUs, from the Web Manager and the OSD. Any user who has administration privileges can turn on, turn off, cycle (reboot), lock, and unlock the outlets. See “Options for Managing Power” on page 43 for a detailed description of how authorized users can manage power. See “Setting Up and Configuring Power Management” on page 42 for a list of the administrative tasks involved in setting up power management.

The following section gives instructions on managing power through the OSD while connected locally to the KVM/net.

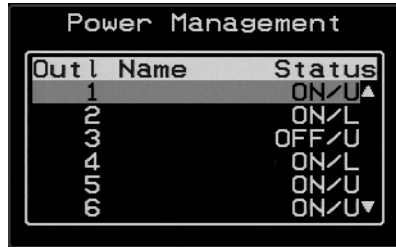
For instructions on how to manage power remotely through the Web Manager, see Table 5-1 on page 273 for a list the power management tasks available to regular users through the Web Manager and links to the associated procedures.

For instructions on managing power servers while connected to them through KVM ports, see “To Power On, Power Off, or Reboot the Connected Server” on page 301.

▼ **To Power On, Power Off, Lock, Unlock, or Cycle Devices Plugged into PM Outlets**

1. Go to: Configure > Power Management.

The Outlet Status page appears with a list of all configured IPDUs. The status column displays whether the outlet is on or off, locked, or unlocked.



Outl Name	Status
1	ON/U▲
2	ON/L
3	OFF/U
4	ON/L
5	ON/U
6	ON/U▼

The letter U displayed in the status window indicates that the outlet is unlocked; the letter L indicates that the outlet is locked.

2. Use the up or down arrow keys to select the outlet you want to edit and press <Enter>.

The Outlet Status window for the selected outlet appears with the current status listed in the Status box and the available action items listed at the bottom.



The available action options at the bottom of the window change depending on the status of the outlet. For example, an outlet that is locked displays only the Unlock option as in the following figure.



An outlet that is turned off and unlocked displays the On, Lock, and Cycle options as in the following figure.



3. Use the arrow keys to select On, Off, Lock, Unlock, or Cycle and press <Enter>.
4. Select the arrow button and press <Enter> to return to the Power Management menu.
5. To change the status of other outlets, repeat steps 2 and 3.

Modem Connections

In addition to connecting to the KVM/net through a regular Ethernet connection, you can also access the KVM/net by dialing in through an installed external modem. Use PPP when dialing into any of the supported modems. Once the connection is made, all connections to the specified IP address are made through the PPP connection. For example, if you enter the specified IP address in a browser after making the PPP connection, the browser connects to the KVM/net through the dialup connection. This way you can access the Web Manager through PPP even if the IP connection to the KVM/net is not available.

The KVM/net administrator performs the procedures to install and configure the modems. Contact your KVM/net administrator for the phone numbers, usernames, and passwords to use, and for questions about how the modems are configured.

Before anyone can use PPP to access the KVM/net, the PPP connection must be configured by the user on the remote computer so the connection can be used for dialing in. Before configuring PPP, you need the following:

- A modem connected to the remote computer.
- The phone number of the line that is dedicated to the KVM/net modem you want to access.
- If authentication is required for the modem, you need a username and password for a user account on the KVM/net.

The following table lists the related procedures and where they are documented.

Table 6-6: Tasks for Configuring and Making Dial Up Connections (User)

Configure a PPP Connection	“To Configure a PPP Connection on a Remote Computer” on page 313
Connect Using PPP	“To Make a PPP Connection From a Remote Computer” on page 314

▼ **To Configure a PPP Connection on a Remote Computer**

Perform this procedure on a remote computer with a modem to do the following:

- Create a PPP connection that anyone can use for dialing up the KVM/net
- Optionally configure call back.

See the prerequisites listed in “Modem Connections” on page 312, if needed.

Note: The following steps work for a computer running Windows XP. The steps are different on computers running other Windows versions or other operating systems. You can use this procedure as an example.

1. From “My Computer,” go to “My Network Places.”
2. Under “Network Tasks,” click “View network connections.”
3. Under “Network Tasks,” select “Create a new connection.”
The “New Connection Wizard” appears.
4. Click the “Next” button.
5. Click “Connect to the Internet” and click “Next>.”
The “Getting Ready” form appears.
6. Click “Set up my connection manually” and click “Next>.”
The “Internet Connection” form appears.
7. Click “Connect using a dial-up modem” and click “Next>.”
The “Connection Name” form appears.
Type a name for the connection to the KVM/net in the “ISP Name” field and click “Next>.”
The “Phone Number to Dial” form appears.
8. Type the phone number for the KVM/net’s modem in the “Phone number” field and click “Next>.”
The “Internet Account Information” form appears.
9. Type the username for accessing the KVM/net in the “User name” field.

Accessing Connected Devices

10.Type the password for accessing the KVM/net in the “Password” and “Confirm Password” field and click “Next>.”

11.Click the “Finish” button.

The “Connect *connection_name*” dialog appears.

12.Click the “Cancel” button.

The name of the connection appears on the Network Connections” list.

13.To configure call back, do the following steps.

a. Select the name of the connection from the Network Connections dialog box.

b. Select “Dial Up Preferences” from the “Advanced” menu.

The “Dial-up Preferences” dialog box appears.

c. Click the “Callback” tab.

d. Click “Always call me back at the number(s) below.”

e. Highlight the name of the modem and click “Edit.”

The “Call Me Back At” dialog box appears.

f. Enter the phone number of your local modem in the “Phone number:” field, and click OK.

▼ **To Make a PPP Connection From a Remote Computer**

Perform this procedure on a remote computer that has a modem to initialize a dial up and optional call back session on the KVM/net. This procedure assumes a PPP connection for dial up or call back has previously been created as described in “To Configure a PPP Connection on a Remote Computer” on page 313.

Note: The following steps work if you are on a computer running Windows XP. The steps are different on computers running other Windows versions or other operating systems, but you can use these steps as an example.

1. From the Start menu, go to My Computer>My Network Places.

2. Under “Network Tasks,” click “View network connections.”

3. Double-click the name of the connection in the list.

The “Connect *connection_name*” dialog appears.

4. Type the username and password in the “User Name” and “Password” fields.
5. Click the “Dial” button

Accessing Connected Devices

Chapter 7

On Screen Display

This chapter provides an overview of the on screen display (OSD). Most configuration and operations tasks are performed through the Web Manager, as described in Chapter 5 and Chapter 4. Administrators and operators can use the OSD for troubleshooting when a direct connection method is required.

Access to the OSD requires a local keyboard, monitor, and mouse connected to the KVM management ports, User 1 or User 2, on the back of the KVM/net. See “To Connect to the User 1 Management Port” on page 75 for instructions on connecting to the User 1 port, or see “To Connect the RP to the KVM/net” on page 120 for instructions on connecting to the User 2 port.

Once the connected monitor is turned on, the OSD login window appears.

Navigating the OSD

In the OSD you can use keyboard sequences to navigate the windows and make menu selections. The following sections describe:

- Basic Navigation Keys
- Common Navigation Actions

Basic Navigation Keys

The following table displays a short list of keyboard controls to help you navigate the KVM/net on screen display. The OSD window must be selected and in an *active* state for these keys to work.

Table 7-1: Basic Navigation Keys

Key	Action
Tab	Changes between fields on the window
Up / Down	Scrolls within a menu
Left / Right	Selects a button in a button field
Backspace	Deletes the character left to the cursor
Page Up / Page Down	Pages within a menu
End	Moves to the end of a menu
Home	Moves to the top of a menu
Enter	Selects highlighted item / Commits changes
Esc	Returns to the previous main menu

Common Navigation Actions

Table 7-2 shows how to perform common actions used to go to windows, select items, and commit changes in the OSD.

Table 7-2: OSD Equivalents for Common Actions

Action	OSD Equivalent
Select OK	Tab to the OK button and press the Enter key on your keyboard.
Save changes	Tab to the Save button and press the Enter key.
Select an option	Tab to the option and press the Enter key.
Go to a specific window, as in: Go to Configure>Users and Groups.	Select the first option from the Main menu. On the next window that comes up select the next option from that menu. Do this until you get to the last option in the menu path.

Logging In Through the OSD

In order to log in to the KVM/net through the OSD, you need to connect a keyboard, monitor, and mouse to the monitor, keyboard, mouse connectors, labelled User 1, on the KVM/net. See “To Connect to the User 1 Management Port” on page 75 for more information.

Optionally, you can connect to the OSD using an AlterPath Remote Presence (RP), which you buy separately. See “Installing the AlterPath KVM Remote Presence” on page 118 for instructions on installing the RP. See “Controlling the OSD Through the AlterPath Remote Presence” on page 387 for instructions on using the RP.

On Screen Display

▼ To Log In to the KVM/net Through the OSD

1. Type your username followed by your password.



2. Press <Enter>.

The main menu of the KVM/net OSD appears. See the following section, “OSD Main Menu” on page 320 for a description of the OSD Main Menu items.

OSD Main Menu

The OSD Main Menu provides six menu selections as depicted in the following figure.

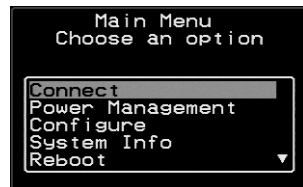


Figure 7-1: OSD Main Menu

Table 7-5 gives a brief description of each menu item and lists where you can find more information.

Table 7-3: OSD Main Menu Items

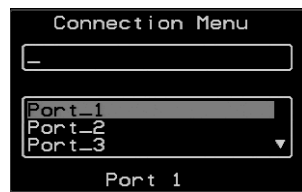
Menu Selection	Select the menu item to:	Where Documented
Connect	View the Server Connection Menu and select the port to which you want to connect.	Page 321

Table 7-3: OSD Main Menu Items

Menu Selection	Select the menu item to:	Where Documented
Power Management	View status of all outlets on connected IPDUs and power on, power off, and cycle connected devices.	Page 322
Configure	View the Configuration Menu and perform KVM/net configuration.	Page 323
System Info	View the system information pertaining to the KVM version that you are using.	Page 385
Reboot	Reboot the KVM/net.	Page 386
Exit	Exit from the OSD and close the session.	N/A

Connection Menu

Administrators and authorized regular users can use the Connection Menu, as displayed in the following figure, to connect to and control servers that are physically connected to KVM ports on the master KVM/net or on any cascaded KVM device.



See “To Connect to Servers Through the OSD Connection Menu” on page 293 for instructions on connecting to servers through the OSD.

Power Management Menu

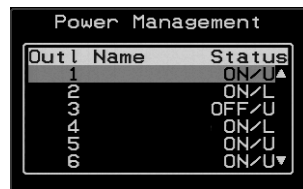
The Power Management windows allow you to check the status of the master IPDU connected to the AUX port in addition to all cascaded IPDUs. Any user who has administration privileges can turn on, turn off, cycle (reboot), lock, and unlock the outlets. See “Connecting AlterPath PMs to the KVM/net” on page 106 for instructions on connecting IPDUs to the KVM/net.

For instructions on managing power through the OSD, see

▼ **To Power On, Power Off, Lock, Unlock, or Cycle Devices Plugged into PM Outlets**

1. Go to: Configure > Power Management.

The Outlet Status page appears with a list of all configured IPDUs. The status column displays whether the outlet is on or off, locked, or unlocked.



Outl Name	Status
1	ON/U▲
2	ON/L
3	OFF/U
4	ON/L
5	ON/U
6	ON/U▼

The letter U displayed in the status window indicates that the outlet is unlocked; the letter L indicates that the outlet is locked.

2. Use the up or down arrow keys to select the outlet you want to edit and press <Enter>.

The Outlet Status window for the selected outlet appears with the current status listed in the Status box and the available action items listed at the bottom.



The available action options at the bottom of the window change depending on the status of the outlet. For example, an outlet that is locked displays only the Unlock option as in the following figure.



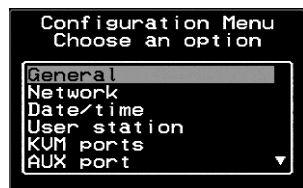
An outlet that is turned off and unlocked displays the On, Lock, and Cycle options as in the following figure.



3. Use the arrow keys to select On, Off, Lock, Unlock, or Cycle and press <Enter>.
4. Select the arrow button and press <Enter> to return to the Power Management menu.
5. To change the status of other outlets, repeat steps 2 and 3.

Configure Menu Overview

Selecting “Configure” from the OSD Main Menu brings up the Configuration Menu. The Configuration Menu provides a number of options, as shown in the following screen.



Not all the options are visible. Table 7-4 gives a brief description of all the menu options and lists where you can find more information

Table 7-4: Configuration Menu Items

Menu Selection	Select the menu item to:	Where Documented
General	Configure authentication type for direct logins to KVM ports; syslog facility number; KVM connection hot key escape sequence, and Sun Keyboard emulation hot key escape sequence. Note: syslogging also requires configuration of the syslog server using the Syslog option, described later in this table.	“General Configuration Screens [OSD]” on page 327
Network	Configure DHCP or assign an IP address and configure other basic network parameters; configure SNMP, VPN, IP filtering, hosts, and static routes	“Network Configuration Menu Options [OSD]” on page 330
Date/Time	Enable/disable NTP or manually configure the system date and time.	“Date/time Configuration Screens” on page 353
User Station	Configure the Local User station’s idle timeout, screen saver time, cycle time, keyboard type, and the various escape sequences for the current workstation.	“User Station Screens” on page 354
KVM Ports	Activate KVM ports, assign aliases, and enable power management.	“KVM Ports Screens” on page 358
AUX Port	Configure the AUX port for PPP or power management.	“AUX Port Screens” on page 359
Users and Groups	Configure users and groups, user passwords, and KVM port access permissions.	“Users and Groups Screens” on page 366
Cascade Devices	Add, edit, or delete configurations of cascaded (slave) KVM units.	

Table 7-4: Configuration Menu Items (Continued)

Menu Selection	Select the menu item to:	Where Documented
Syslog	Configure the IP address of the syslog server. Note: syslogging also requires assignment of a facility number using the General option, described earlier in this table.	“Syslog Screens” on page 373
Authentication	Configure an authentication method for logins to the KVM/net and authentication servers for KVM/net and KVM port logins.	“Authentication Screens” on page 374
Save/Load Config	Permanently save configuration changes, load a stored configuration or restore the configuration to factory default values.	“System Info Menu” on page 385
Exit	Exit from the menu.	N/A

Understanding OSD Configuration Screen Series

Selecting an option from the “Configure” menu usually brings you through a series of related screens, which you navigate through one at a time until you reach the final screen.

For example, if you select Date/Time, you are presented with a series of “Date/time Config.” screens starting with “NTP” and ending with “Time,” as shown in the following figure.



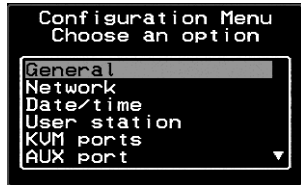
Figure 7-2: First, Middle, and Last Screens in Configuration Series

As illustrated, all the configuration screens except the final screen have a right arrow at the bottom right that you can select to go to the next screen. Clicking “Save” on any one of the screens saves the changes made to that point. You can wait until you get to the final screen in a series before saving changes. Clicking “Save” on the final screen saves any change you have made and takes you back to the Configuration menu.

See “Navigating the OSD” on page 318, if needed, for how to use the Tab key and other keys to move around the screens in the OSD.

General Configuration Screens [OSD]

You can select the General option on the OSD Configuration Menu to configure several general features of the KVM/net, which are introduced under “General” on page 324.



Selecting Configure>General from the OSD Main Menu brings up the Authentication type screen, which is the first in a series of configuration screens that appear in the sequence shown in the following table.

Table 7-5 gives a brief description of the sequence of General configuration screens.

Table 7-5: General Configuration Screens [OSD]

Screen	Description
<p>Authentication Type</p>	<p>The authentication type applies to <i>direct KVM port logins from the KVM/net login screen</i>: None, Local, Radius, TacacsPlus, Kerberos, LDAP, RadiusDownLocal, TacplusDownLocal, KerberosDownLocal, LdapDownLocal, NTLM(Win NT/2k/2k3), NTLMDownLocal, and Windows NT/2K/2K3. Direct logins to KVM ports must also be enabled. (See “Direct Access” on page 328.) You also must ensure that an authentication server is specified for the type of method you select. See “Authentication Screens” on page 374.</p>
<p>Syslog Facility</p>	<p>The syslog facility number that is used by the administrator of the syslog server to identify messages generated by devices connected to the KVM ports. Obtain the facility number to use for the KVM/net from the syslog server’s administrator. Values are from 0 through 7. See “Syslog Servers” on page 49 for examples of using facility numbers as needed. In addition, the IP address of the syslog server must be configured, as described under “Syslog Screens” on page 373.</p>

Table 7-5: General Configuration Screens [OSD] (Continued)

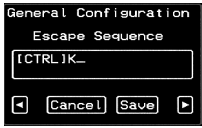
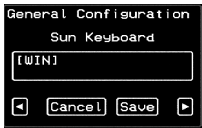
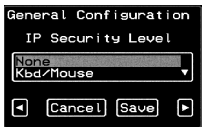

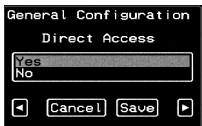
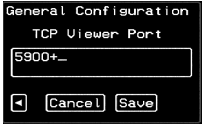
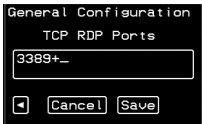
Screen	Description
<p>Escape Sequence</p> 	<p>The escape sequence for AlterPath Viewer hot keys [Default: Ctrl+k, shown as [CTRL]K in the screen]. See “Redefining KVM Connection Hot Keys” on page 37 for more details.</p>
<p>Sun Keyboard</p> 	<p>The escape key for Sun hot keys. Default = the Windows [WIN] key, which is the key with the Windows logo on it. Other options are: [CTRL], [SHIFT], and [ALT]. See “Redefining Sun Keyboard Equivalent Hot Keys” on page 37 for more details.</p>
<p>IP Security Level</p> 	<p>The level of encryption: “None,” “encrypt keyboard and mouse data,” or “encrypt data from the keyboard, video, and mouse.”</p>
<p>3DES</p> 	<p>Disables or enables 3DES encryption.</p>
<p>Direct Access</p> 	<p>Enables or disables direct access to KVM ports from the Web Manager login screen.</p>

Table 7-5: General Configuration Screens [OSD] (Continued)

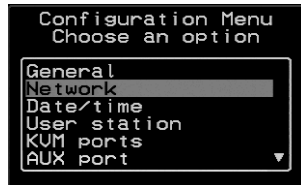
Screen	Description
TCP Port Viewer 	Allows you to assign an alternate TCP Port number or numbers for the AlterPath Viewer to use [Default, 5900+]. Use the plus sign (+) to increment the port number by 1 for each additional AlterPath Viewer. For example: 5903+ means that the first AlterPath Viewer uses port 5903 and the second uses port 5904. Use the hyphen (-) to indicate a range of addresses, for example, 5903-5907. Use the comma (,) to separate two TCP port addresses, for example, 5901,5903. Combine commas and hyphens, as desired, for example: 1901,5903-5905,5907. Note: Do not use reserved port numbers 1 through 1024.
TCP RDP Ports 	Specify the TCP ports or a range of TCP ports to be used for RDP (in-band) server connections. You must have at least eight valid TCP ports specified in order to have up to eight simultaneous in-band connections through the KVM/net. For example, if you want ports 3389 to ports 10000 to be used, type “3389 - 10000”. If you want to use ports 3389 and higher, type “3389+”. If you want to use ports 3389 and below, type “3389-”. You can request valid TCP ports from your network administrator.

Note: The Save button on every screen saves configuration changes into the configuration files. To permanently save the configuration changes, you must select Save/Load Conf. from the Configuration Menu.

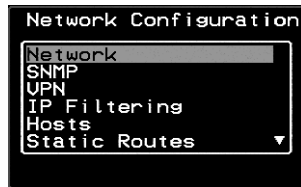
On Screen Display

Network Configuration Menu Options [OSD]

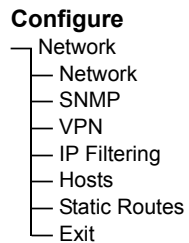
You can select the Network option on the OSD Main Menu to configure network-related services for the KVM/net.



Selecting Network under Configuration brings up the Network Configuration Menu. The Network Configuration Menu provides a number of options, as shown in the following screen.



Not all the options are visible. The following diagram lists the names of all the configuration options accessed from the Configure>Network menu.

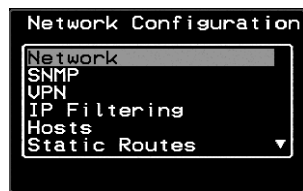


The configuration screen series for each of the options under Configure>Network are listed and described in the following sections:

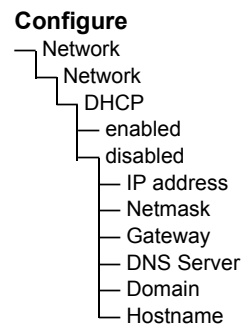
Network Configuration Screens [OSD]	Page 331
SNMP Configuration Screens [OSD]	Page 334
VPN Configuration Screens [OSD]	Page 338
IP Filtering Configuration Screens	Page 342
Hosts Configuration Screens [OSD]	Page 349
Static Routes Configuration Screens	Page 350

Network Configuration Screens [OSD]

You can select the Network option from the Network Configuration menu to configure DHCP or configure a fixed IP address and other basic network parameters.



The following diagram lists the names of the configuration screens accessed under Configure>Network>Network.



On Screen Display

Selecting Configure>Network>Network from the OSD Main Menu brings up the DHCP screen, which is the first in a series of configuration screens that appear in the sequence shown in the following table.

Table 7-6 gives a description of all the related configuration screens.

Table 7-6: Network Configuration Screens [OSD]

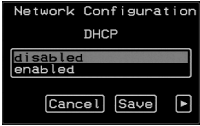
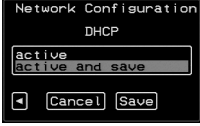
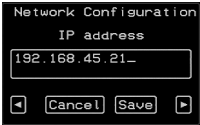
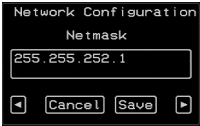
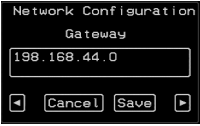
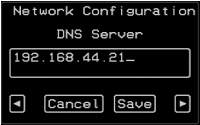

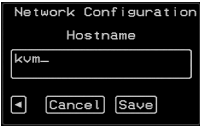
Screen	Description
DHCP 	Enable or disable DHCP. When you select “enabled,” the screen shown in the following figure appears.
	“active” saves the changes to the configuration files. “active and save” overwrites the backup configuration files and makes the changes permanent. Either choice brings you back to the Network Configuration menu.
IP Address 	When “disabled” is selected, the IP address, Netmask, Gateway, DNS Server, Domain, and Hostname forms appear in the sequence shown in the following rows. The IP address of the KVM/net.
Netmask 	The netmask for the subnet (if applicable) in the form <i>NNN.NNN.NNN.N</i> (for example: 255.255.252.0).

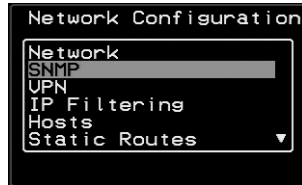
Table 7-6: Network Configuration Screens [OSD] (Continued)

Screen	Description
Gateway 	The IP address for the gateway (if applicable).
DNS Server 	The IP address for the DNS server.
Domain 	The domain name.
Hostname 	The hostname for the KVM/net.

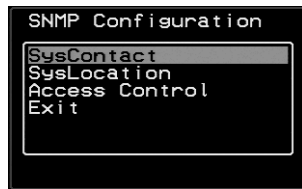
On Screen Display

SNMP Configuration Screens [OSD]

You can select the SNMP option from the Network Configuration menu to configure SNMP.

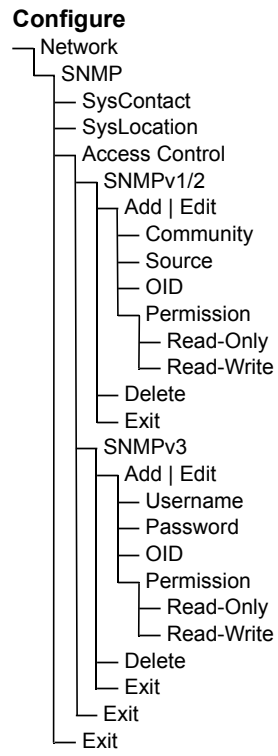


Selecting SNMP under Configuration>Network brings up the SNMP Configuration Menu. The SNMP Configuration Menu provides a number of options, as shown in the following screen.



The following diagram lists the names of all the configuration screen series accessed from the Configure>Network>SNMP Configuration menu.

The following diagram lists the names of the configuration screens accessed under Configure>Network>SNMP.



On Screen Display

Table 7-7 gives a brief description of all the SNMP configuration screens.

Table 7-7: SNMP Configuration Screens [OSD]

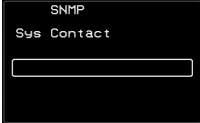
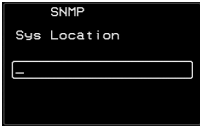
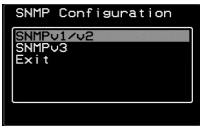



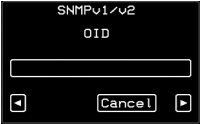
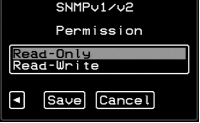


Screen	Description
SysContact 	The email address for the KVM/net administrator, for example: <code>kvm_admin@cyclades.com</code> .
SysLocation 	The physical location of the KVM/net.
Access Control 	Choices are SNMP v1/2 or SNMP v3.
SNMP Configuration 	Appears when either SNMP v1/2 or SNMP v3 is selected. Choices are “Add,” “Edit/Delete,” or “Exit.”
SNMPv1/v2 Community 	The community name is sent in every SNMP communication between the client and the server, and the community name must be correct before requests are allowed. Communities are further defined by the type of access specified under “Permission”: either read only or read write. The most common community is “public” and it should not be used because it is so commonly known. By default, the public community cannot access SNMP information on the KVM/net.

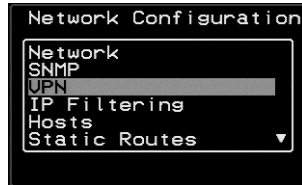
Table 7-7: SNMP Configuration Screens [OSD] (Continued)

Screen	Description
<p>SNMPv1/v2 Source</p> 	<p>The source IP address or range of IP addresses.</p>
<p>SNMPv1/v2 or v3 OID</p> 	<p>Object Identifier. Each managed object has a unique identifier.</p>
<p>SNMPv1/v2 or v3 Permission</p> 	<p>Choices are “Read-Only” and “Read-Write.”</p> <p>Read Only - Read-only access to the entire MIB (Management Information Base) except for SNMP configuration objects.</p> <p>Read/Write - Read-write access to the entire MIB except for SNMP configuration objects.</p>
<p>SNMPv3 Username</p> 	<p>User name.</p>
<p>SNMPv3 Password</p> 	<p>Password.</p>

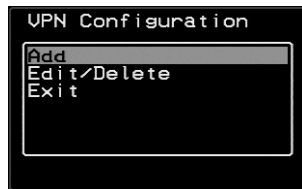
On Screen Display

VPN Configuration Screens [OSD]

You can select the VPN option from the Network Configuration menu to configure VPN.



Selecting VPN under Configuration>Network brings up the VPN Configuration Menu. The VPN Configuration Menu provides the options shown in the following screen.



You can use these options to add a VPN connection or to edit or delete a previously-configured VPN connection. See “VPN” on page 227 for details.

The following diagram lists the names of the configuration screens accessed from the Add and Edit/Delete options on the Configure>Network>VPN Configuration menu.

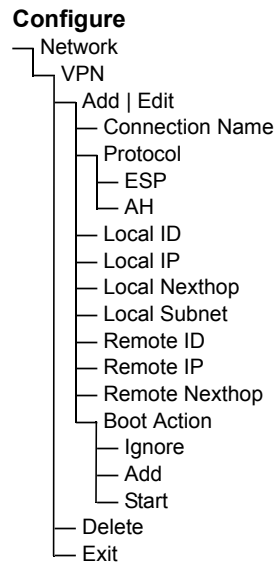
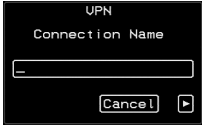
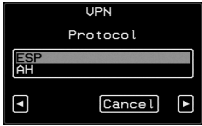


Table 7-8 gives a brief description of the VPN configuration screens series under Add and Edit.

Table 7-8: VPN Configuration Screens [OSD]

Screen	Description
<p>Connection Name</p> 	Any descriptive name you want to use to identify this connection such as “MYCOMPANYDOMAIN-VPN”
<p>Protocol</p> 	The authentication protocol used, either “ESP” (Encapsulating Security Payload) or “AH” (Authentication Header)

On Screen Display

Table 7-8: VPN Configuration Screens [OSD] (Continued)

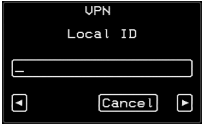
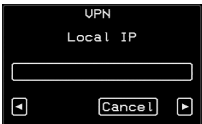

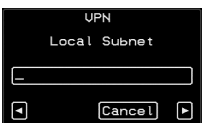
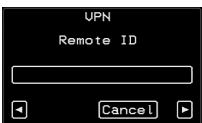

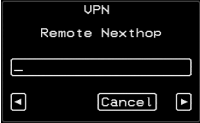
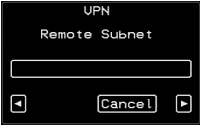
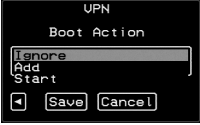
Screen	Description
Local ID 	The hostname of the KVM/net, referred to as the “local” host.
Local IP 	The IP address of the KVM/net.
Local NextHop 	The router through which the KVM/net sends packets to the host on the other side.
Local Subnet 	The netmask of the subnetwork where the KVM/net resides, if applicable.
Remote ID 	The hostname of the remote host or security gateway
Remote IP 	The IP address of the remote host or security gateway.

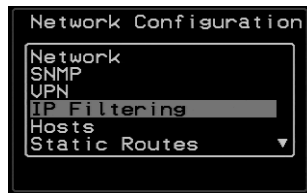
Table 7-8: VPN Configuration Screens [OSD] (Continued)

Screen	Description
<p>Remote Nexthop</p> 	The IP address of the router through which the host on the other side sends packets to the KVM/net.
<p>Remote Subnet</p> 	The netmask of the subnetwork where the remote host or security gateway resides, if applicable.
<p>Boot Action</p> 	Choices are “Ignore,” “Add,” and “Start.” “Ignore” means that VPN connection is ignored. “Add” means to wait for connections at startup. “Start” means to make the connection

On Screen Display

IP Filtering Configuration Screens

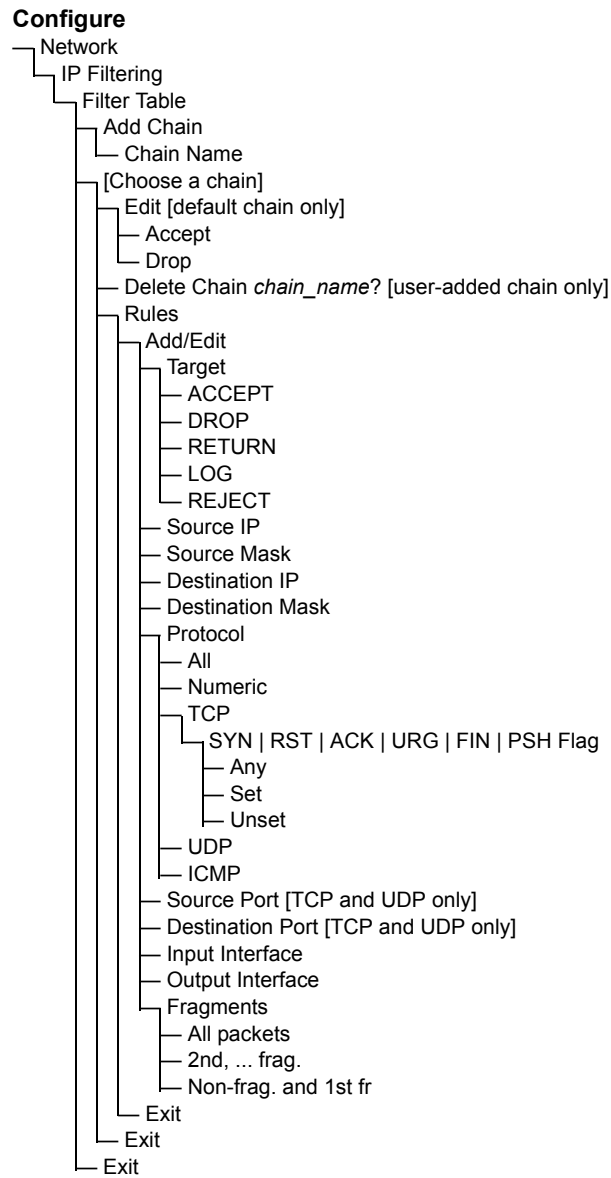
You can select the IP Filtering option from the Network Configuration menu to configure the KVM/net to filter packets like a firewall. See “Packet Filtering on the KVM/net” on page 39 for details.



Selecting IP Filtering under Configuration>Network brings up the “Filter Table.” The “Filter Table” lists the default chains along with any administratively-configured chains, the “Add Chain,” and the “Exit” options, as shown in the following screen.



You can use this menu to create chains and set up rules for the new chains or you can edit or delete a previously-configured chain. The following diagram lists the names of the configuration screens accessed under Configure>Network>IP Filtering.



On Screen Display

The following table shows the IP filtering screens.

Table 7-9: IP Filtering Configuration Screens [OSD]



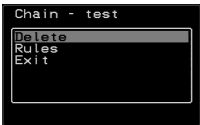

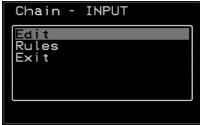
Screen	Description
Filter Table 	Lists the default chains along with any administratively-configured chains, the “Add Chain,” and the “Exit” options.
Chain Name 	Only appears when “Add Chain” is selected. Entering the name of the chain adds the new chain’s name to the “Filter Table,” where you need to select the name of the new chain and define rules for the chain.
Chain - <i>chain_name</i> 	Appears when a user-added chain is selected from the “Filter Table.” The choices are “Delete,” “Rules,” “Exit.”
Delete Chain <i>chain_name</i>? 	Appears when a user-added chain is selected and the Delete option is chosen from the “Chain - <i>chain_name</i> ” menu.
Chain - <i>CHAIN_NAME</i> 	Appears when a default chain is selected from the “Filter Table.” The choices are “Edit,” “Rules,” and “Exit.”

Table 7-9: IP Filtering Configuration Screens [OSD] (Continued)

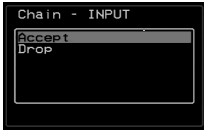
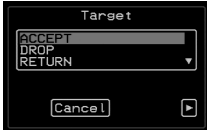
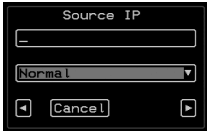

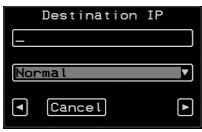
Screen	Description
<p>Edit</p> 	<p>Appears when a default chain is selected and the Edit option is chosen from the Chain - <i>Chain_name</i> menu. Choices are “Accept” or “Drop.”</p>
<p>Target</p> 	<p>The following screens define the rules for packet filtering. The packet is filtered for the characteristics defined in the rule, for example, a specific IP header, input and output interfaces, TCP flags or protocol. The target action is performed on all packets that have the characteristic. If “Inverted” is selected for a characteristic, the target action is performed on all packets that do not have the characteristic.</p> <p>Appears when a user-added chain is selected. Choices specify the target action to take when a packet’s characteristics match the rule, or, if “Inverted” is selected, if the packets do not match the rule. Choices are: “ACCEPT,” “DROP,” “RETURN,” “LOG,” and “REJECT.”</p>
<p>Source IP</p> 	<p>The IP address of the source of an input packet.</p>
<p>Source Mask</p> 	<p>The netmask of the subnetwork where an input packet originates.</p>
<p>Destination IP</p> 	<p>The IP address of an output packet’s destination.</p>

Table 7-9: IP Filtering Configuration Screens [OSD] (Continued)


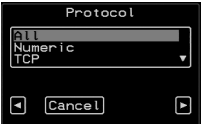
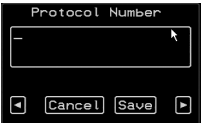
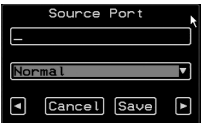
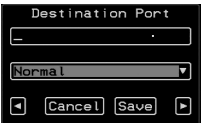

Screen	Description
<p>Destination Mask</p> 	<p>The netmask of the subnet to which an output packet is going.</p>
<p>Protocol</p> 	<p>Choices are “All,” “Numeric,” “TCP,” “UDP,” “ICMP.”</p>
<p>Protocol Number</p> 	<p>Appears only if “Numeric” is selected from the “Protocol” menu.</p>
<p>Source Port</p> 	<p>Appears only if “TCP” or “UDP are selected from the “Protocol” menu. The source port number.</p>
<p>Destination Port</p> 	<p>Appears only if “TCP” or “UDP are selected from the “Protocol” menu. The destination port number.</p>
<p>SYN Flag</p> 	<p>Appears only if “TCP” is selected from the “Protocol” menu. Options are “Any,” “Set,” “Unset.”</p>

Table 7-9: IP Filtering Configuration Screens [OSD] (Continued)









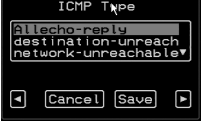
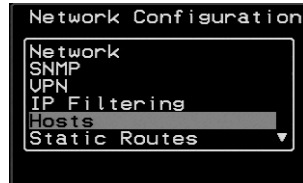
Screen	Description
<p>RST Flag</p> 	<p>Appears only if “TCP” is selected from the “Protocol” menu. Options are “Any,” “Set,” “Unset.”</p>
<p>ACK Flag</p> 	<p>Appears only if “TCP” is selected from the “Protocol” menu. Options are “Any,” “Set,” “Unset.”</p>
<p>URG Flag</p> 	<p>Appears only if “TCP” is selected from the “Protocol” menu. Options are “Any,” “Set,” “Unset.”</p>
<p>FIN Flag</p> 	<p>Appears only if “TCP” is selected from the “Protocol” menu. Options are “Any,” “Set,” “Unset.”</p>
<p>PSH Flag</p> 	<p>Appears only if “TCP” is selected from the “Protocol” menu. Options are “Any,” “Set,” “Unset.”</p>
<p>Input Interface</p> 	<p>Appears only if “All,” “Numeric,” “TCP,” “UDP,” or “ICMP” are selected from the “Protocol” menu.</p>

Table 7-9: IP Filtering Configuration Screens [OSD] (Continued)

Screen	Description
<p>Output Interface</p> 	<p>Appears only if “All,” “Numeric,” “TCP,” “UDP,” or “ICMP” are selected from the “Protocol” menu.</p>
<p>Fragments</p> 	<p>Appears only if “All,” “Numeric,” “TCP,” “UDP,” or “ICMP” are selected from the “Protocol” menu.</p>
<p>ICMP Type</p> 	<p>Appears only if ICMP is selected from the “Protocol” menu. Choices are:</p> <ul style="list-style-type: none"> • all • echo-reply • destination-unreachable • network-unreachable • host-unreachable • port-unreachable • fragmentation needed • source-route-failed • network-unknown • host-unknown • network-prohibited • host-prohibited

Hosts Configuration Screens [OSD]

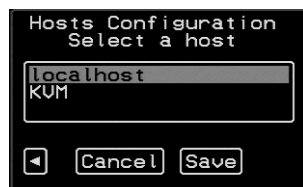
You can select the Hosts option from the Network Configuration menu to configure hosts.



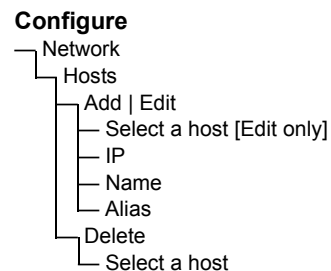
Selecting Hosts under Configuration>Network brings up the “Hosts List” action menu, as shown in the following screen.



You can select the options on this menu to add, edit, or delete host entries. Selecting “Edit” or “Delete Entry” brings up the following “Select a host” screen.



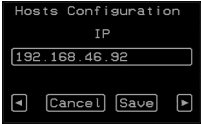
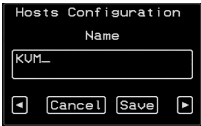

The following diagram lists the names of the configuration screens accessed under Configure>Network>Hosts.



On Screen Display

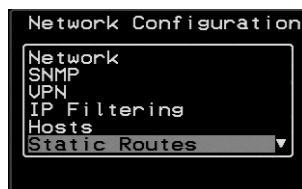
The following table shows the screens for the Add and Edit options.

Table 7-10: Hosts Configuration Screens [OSD]

Screen	Description
IP 	IP address of the host
Name 	Hostname of the host
Alias 	Optional alias of the host

Static Routes Configuration Screens

You can select the Static Routes option from the Network Configuration menu to configure static routes.

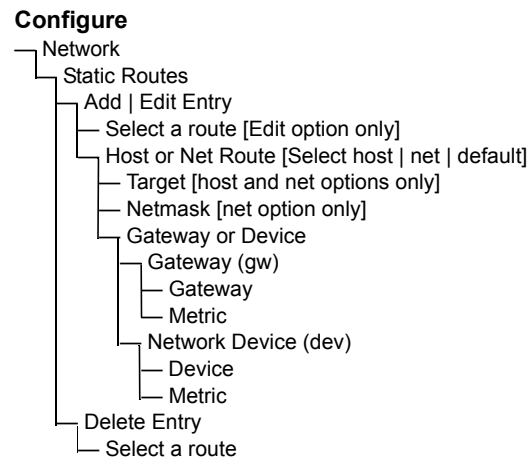


If judiciously used, static routes can sometimes reduce routing problems and routing traffic overhead. If injudiciously used, when a network fails, static routes can block packets that would otherwise be able to find alternate routes around the point of failure if dynamic-routing were in effect.

Selecting Static Routes under Configuration>Network brings up the Static Routes Action Menu, as shown in the following screen.



The following diagram lists the names of the configuration screens accessed under Configure>Network>Static Routes.



The following table shows the static routes screens that appear when you select one of the actions.

Table 7-11:Static Routes Screens [OSD]

Screen	Description
<p>Select a route</p>	<p>Appears only when the Edit and Delete options are selected. Choices are “default” and any previously-configured static routes.</p>

On Screen Display

Table 7-11:Static Routes Screens [OSD] (Continued)

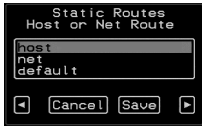
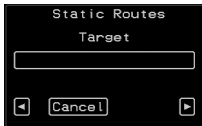




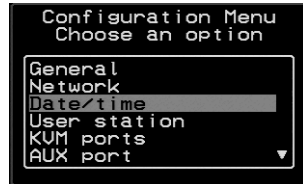
Screen	Description
Host or Net Route 	Types of routes: “host,” “net,” or “default.” Note: A default route is used to direct packets that are addressed to networks not listed in the routing table.
Target 	IP address for the target host or network.
Netmask 	Appears only when “net” is selected from the “Host or Net Route” screen. Netmask for the destination.
Gateway or Device 	Two options are: “Gateway (gw)” or “Network Device (dev).”
Gateway 	Appears only when “Gateway (gw)” is selected from the “Gateway or Device” menu. Gateway IP address.
Device 	Appears only when “Network Device” is selected from the “Gateway or Device” menu. Device address (such as eth0).

Table 7-11:Static Routes Screens [OSD] (Continued)

Screen	Description
Metric 	The number of hops to the destination.

Date/time Configuration Screens

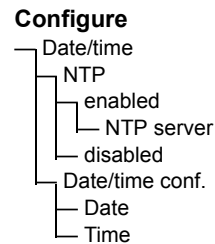
You can select the Date/time option from the OSD Configuration menu to either configure an NTP server or manually set the date and time.



Selecting Date/time under Configuration>Network brings up the NTP menu, as shown in the following screen.



The following diagram lists the names of the configuration options accessed from the Configure>Date/time menu.



On Screen Display

If NTP is enabled, the following screen appears for entering the IP address of the NTP server.

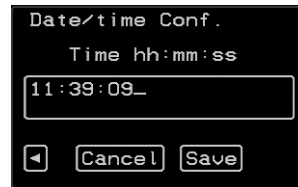


A screenshot of a terminal window titled "Date/time Conf." with the subtitle "NTP server". A text input field contains the IP address "129.6.15.28". Below the input field are three buttons: a left arrow, "Cancel", and "Save".

If NTP is disabled, the following series of two screens appears to allow you to enter the date and time manually.



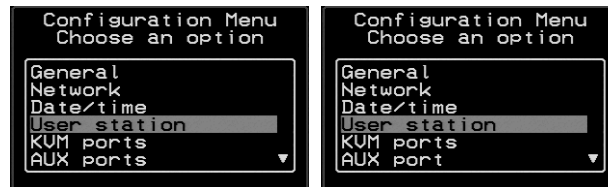
A screenshot of a terminal window titled "Date/time Conf." with the subtitle "Date YYYY/MM/DD". A text input field contains the date "2005/01/25". Below the input field are four buttons: a left arrow, "Cancel", "Save", and a right arrow.



A screenshot of a terminal window titled "Date/time Conf." with the subtitle "Time hh:mm:ss". A text input field contains the time "11:39:09_". Below the input field are three buttons: a left arrow, "Cancel", and "Save".

User Station Screens

You can select the User Station option from the OSD Configuration menu to redefine the parameters that apply to a local user session (when a user is accessing the OSD through the User 1 or User 2 port).



Two side-by-side screenshots of a terminal window titled "Configuration Menu" with the subtitle "Choose an option". The left screenshot shows a list of menu items: "General", "Network", "Date/time", "User station", "KVM ports", and "AUX ports". "User station" is highlighted with a grey bar. The right screenshot shows the same list, but "User station" is no longer highlighted, and "AUX port" is visible at the bottom of the list.

The changes apply only to the currently accessed local station. For example, if an administrator configures these settings while connected to the User 2 port, these settings will be changed for all users who log in to the User 2 port, but the User 1 port setting will remain unchanged.

The following diagram lists the configuration screens accessed through the Configure>User station option. All the screens that appear after the “Keyboard type” screen are for optionally redefining the command key portion of the KVM connection hot keys: “Quit,” “Power Management,” “Mouse/Keyboard Reset,” “Video Configuration,” “Switch Next,” “Switch Previous,” and “Port Info.” See “Redefining Keyboard Shortcuts (Hot Keys)” on page 37 for details, if needed.

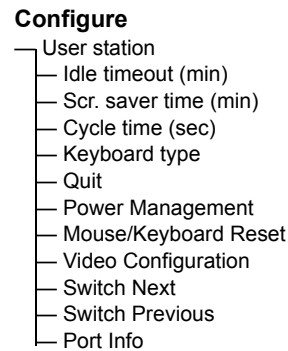


Figure 7-3: User Station Configuration Screens

The following table shows the user station configuration screens.

Table 7-12:User Station Configuration Screens

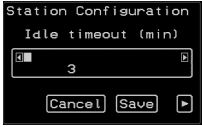
Screen	Description
<p>Idle timeout</p> 	<p>The period of inactivity before the user is logged out from the OSD. The default is 3 minutes.</p>

Table 7-12:User Station Configuration Screens (Continued)

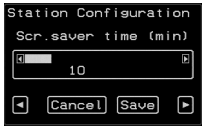
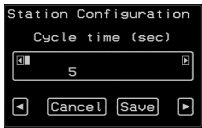

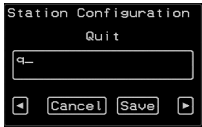
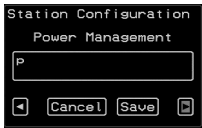
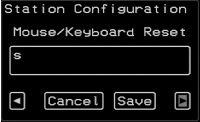
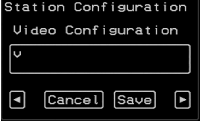
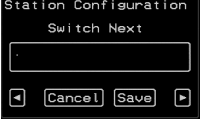
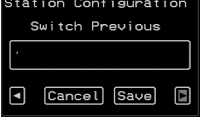
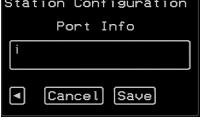
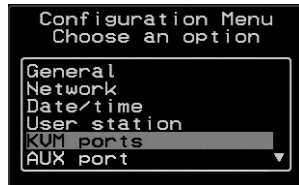
Screen	Description
<p>Scr. saver timeout</p> 	<p>The period of inactivity before the screen saver starts. The default is 10 minutes.</p>
<p>Cycling</p> 	<p>The number of seconds each server is viewed while the user is cycling from one port to another. Default = 5 seconds. See “To Initiate Cycle by Server” on page 298 for instructions on how to cycle through the servers.</p>
<p>Keyboard Type</p> 	<p>The type of keyboard connected to the User 1 or User 2 management port of the KVM/net.</p> <ul style="list-style-type: none"> • US [Default] • BR-ABNT • BR-ABNT2 • Japanese • German • Italian • French • Spanish
<p>Quit</p> 	<p>Redefine the command key for the KVM connection quit hot key.</p>
<p>Power Management</p> 	<p>Redefine the command key portion of the KVM connection power management hot key.</p>

Table 7-12:User Station Configuration Screens (Continued)

Screen	Description
<p>Mouse/Keyboard</p> 	<p>Redefine the command key portion of the KVM connection mouse/keyboard reset hot key.</p>
<p>Video</p> 	<p>Redefine the command key portion of the KVM connection video brightness and contrast hot key.</p>
<p>Switch Next</p> 	<p>Redefine the command key portion of the KVM connection switch next hot key.</p>
<p>Switch Previous</p> 	<p>Redefine the command key portion of the KVM connection switch previous hot key.</p>
<p>Port Info</p> 	<p>Redefine the command key portion of the KVM connection port info hot key.</p>

KVM Ports Screens

You can select the KVM Ports option on the OSD Configuration Menu to configure KVM ports.



The following diagram lists the configuration screens accessed through the Configure>KVM ports option.

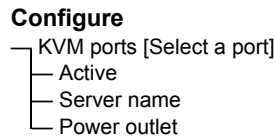



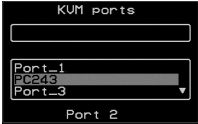
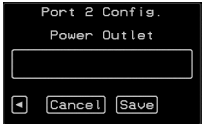
Figure 7-4: KVM Ports Configuration Screens

The following table shows the KVM port configuration screens.

Table 7-13: KVM Port Configuration Screens

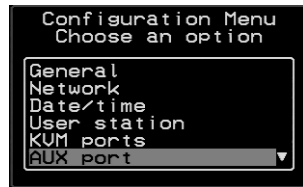
Screen	Description
<p>KVM ports</p>	Lists all KVM ports by their default names or administratively-defined aliases.
<p>Active</p>	Choices are “Yes” and “No” to activate or deactivate the selected KVM port.

Table 7-13:KVM Port Configuration Screens (Continued)

Screen	Description
<p>Server name</p> 	<p>Allows you to assign a descriptive alias, such as the name of the server to which the selected KVM port is connected. Only alpha-numeric characters, hyphens (-), and underscores (_) are accepted. The new alias replaces the default port name in the list of ports as shown here:</p> 
<p>Power Outlet</p> 	<p>Allows you to enter one or more numbers that identify power outlet or outlets into which the server that is connected to this KVM port is plugged.</p> <p>When IPDUs are daisy-chained, the outlets on the second and subsequent IPDUs are numbered sequentially. For example, if two eight-outlet AlterPath PMs are daisy-chained, you would use the number 12 to specify the fourth outlet on the second PM in the chain. You can enter up to twenty characters, so you can specify up to four outlets. See “Controlling Power While Connected to KVM Ports” on page 44 for details. Also see “To Power On, Power Off, or Reboot the Connected Server” on page 301, if needed.</p>

AUX Port Screens

You can select the AUX Port option on the OSD Configuration Menu to configure the AUX port.



The following diagram lists the configuration screens accessed through the Configure>AUX port option.

On Screen Display

Configure

- AUX port [Select a port]
- Active
- Server name
- Power outlet

Figure 7-5: AUX Port Configuration Screens

The following table shows the AUX port configuration screens.

Table 7-14:KVM Port Configuration Screens

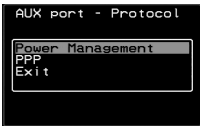


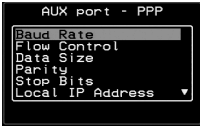
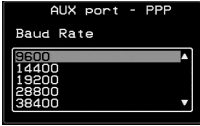

Screen	Description
<p>AUX port - Protocol</p> 	<p>Choices are “Power Management” and “PPP.”</p> <p>If you select Power Management, the following confirmation screen displays:</p>  <p>If you select PPP, the following connection configuration menu displays:</p> 
<p>AUX port - PPP</p> 	<p>Appears when PPP is selected from the AUX port - Protocol screen. Allows you to configure the connection settings for any PPP connection being made through an external modem connected to the AUX port.</p>
<p>AUX port - PPP Baud Rate</p> 	<p>The port speed.</p>

Table 7-14:KVM Port Configuration Screens (Continued)

Screen	Description
AUX port - PPP Flow Control 	Gateway or interface address used for the route.
AUX port - PPP Data Size 	The number of data bits.
AUX port - PPP Parity 	None, even, or odd.
AUX port - PPP Stop Bits 	The number of stop bits.
AUX port - PPP Local IP 	

On Screen Display

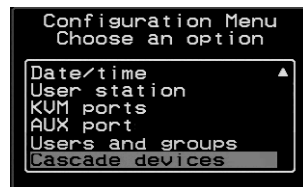
Table 7-14:KVM Port Configuration Screens (Continued)

Screen	Description
AUX port - PPP Remote IP 	

Cascade Devices

You can select the Cascade Devices option on the OSD Configuration Menu to perform the following tasks:

- Add a secondary KVM unit to be cascaded from the master KVM/net.
- Edit the configuration of a cascaded device.
- Delete the configuration of a cascaded device.



The Cascade Devices option of the Configuration Menu allows you to configure a secondary KVM unit to be cascaded to the KVM/net to increase the number of supportable ports. The secondary device may be a KVM/net

Plus, a KVM/net, a KVM, or a KVM Expander. The following diagram lists the configuration screens accessed through the Configure>AUX port option.



Figure 7-6: Cascade Devices Configuration Screens

The following table shows the Cascade Devices configuration screens.

Table 7-15: Cascade Devices Configuration Screens

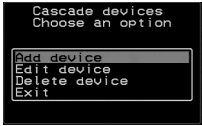


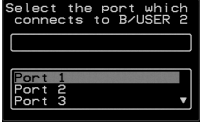
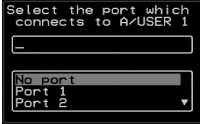
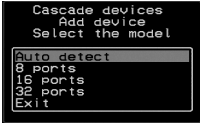
Screen	Description
Cascade device Choose an option 	Options include Add device, Edit device, and Delete device.
Cascade Device Add Device Enter the device name 	Appears when Add device is selected from the “Cascade device Choose an option” screen. Enter the name of the new cascaded KVM unit.

Table 7-15: Cascade Devices Configuration Screens (Continued)

Screen	Description
<p>Cascade Device Edit Device Select the device</p> 	<p>Appears when Edit device is selected from the “Cascade device Choose an option” screen.</p> <p>Select the name of a previously added cascaded KVM unit.</p>
<p>Select the port which connects to B/USER 2</p> 	<p>Enter the port number of the master KVM/net that is connected to the User 2 port of the secondary KVM device or the B port on the Expander.</p> <p>Note: See “Connecting Cascaded KVM Units to the Primary KVM/net” on page 115 for a background on the possible devices that can be cascaded and for instructions on connecting these devices to the master KVM/net.</p>
<p>Select the port which connects to A/USER 1</p> 	<p>Enter the secondary KVM port that is connected to the User 1 port of the primary KVM/net or the User A port on the Expander.</p>
<p>Cascade device Add device Select Model</p> 	<p>Select the number of ports on the cascaded KVM unit or select Auto detect and press <Enter>.</p> <p>Selecting Auto detect automatically detects the number of ports on the cascaded KVM unit. The unit must be already connected in order for the auto detect option to work.</p> <p>During auto detection, the following message appears.</p>

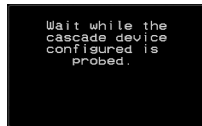




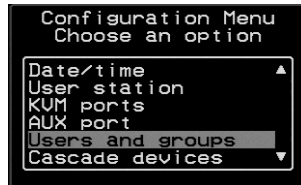
Table 7-15: Cascade Devices Configuration Screens (Continued)

Screen	Description
Cascade Device Delete Device Select the device	Appears when Delete device is selected from the “Cascade device Choose an option” screen.
	The following confirmation screen appears once a cascaded device is selected.
	

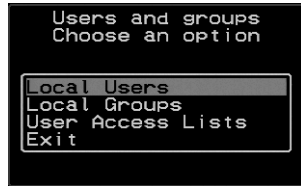
On Screen Display

Users and Groups Screens

You can choose the “Users and groups” option from the OSD Configuration menu to configure users, groups, and KVM port permissions.



When you select “Users and Groups,” the “Choose an option” screen appears, as shown in the following screen example. The “Local Users” option is for configuring users; the “Local Groups” option is for configuring groups, and the “User Access Lists” option is for configuring users’ and groups’ access to KVM ports.



The following diagram lists the configuration screens accessed through the Configure>Users and Groups options:

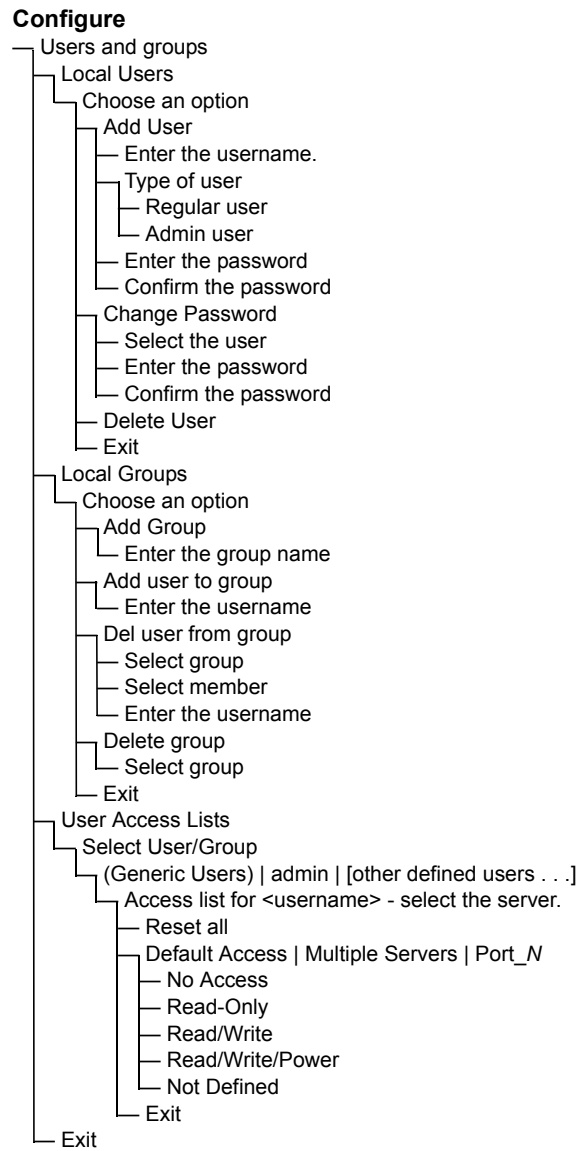


Figure 7-7: Users and Groups Configuration Screens

On Screen Display

The following table shows the configuration screens that appear when the “Local Users” option is selected from the Users and Groups menu under Configure in the OSD.

Table 7-16:Local Users Configuration Screens

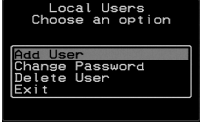
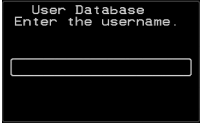




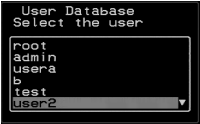

Screen	Description
Choose an option 	Options are: “Add User,” “Change Password,” “Delete User,” or “Exit.”
User Database Enter the username 	Appears only when “Add User” is selected.
Type of user 	Appears only when “Add User” is selected.
Enter the password 	Appears only when “Add User” or “Change Password” are selected. Note: Passwords are case sensitive.
Confirm the password 	When the password is successfully confirmed, the following dialog box appears. 

Table 7-16:Local Users Configuration Screens (Continued)

Screen	Description
<p>Select the user</p> 	<p>Appears only when “Change Password” or “Delete User” are selected. When “Delete User” and then a username are selected, a confirmation screen like the following appears:</p> 

The following table shows the configuration screens that appear when the “Local Groups” option is selected from the Users and Groups menu under Configure in the OSD.

Table 7-17:Local Groups Configuration Screens

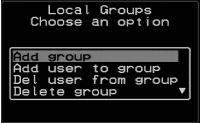
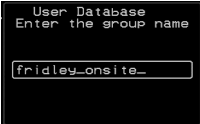

Screen	Description
<p>Choose an option</p> 	<p>Options are “Add group,” “Add user to group,” “Del. user from group,” “Delete group,” and Exit</p>
<p>Enter the group name</p> 	<p>When “Add group” is selected. After the group name is entered, a confirmation screen like the following appears.</p> 

Table 7-17:Local Groups Configuration Screens (Continued)

Screen	Description
<p>Enter the username</p> 	<p>When “Add user” or “Add user to group” are selected. To add multiple users, use a comma to separate each username.</p> <p>When the user is successfully added, the following confirmation screen appears.</p>
<p>Delete user from group select group</p> 	<p>When “Del user from group” is selected.</p>
<p>Select member</p> 	<p>When “Del user from group” and a username are selected, the user is removed from the group, and the following confirmation screen appears:</p>
<p>Delete group select group</p> 	<p>When “Delete group” and a group name are selected, the following confirmation screen appears.</p>

You can use the User Access Lists menu to view and change KVM port access permissions for the Default User and all administratively-configured users and groups. See “Prerequisites for Accessing Servers With KVM Connections” on page 281 for details.

The following table shows the configuration screens related to setting KVM port access permissions when the “User Access List” option is selected from the Users and Groups menu under Configure in the OSD.

Table 7-18:User Access List KVM Port Permissions Configuration Screens

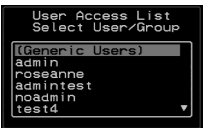
Screen	Description
<p>Select User/Group</p> 	<p>“[Generic Users],” “admin,” and any administratively-defined users and groups are listed, along with the “Exit” option.</p> <p>The Generic Users’ permissions apply to all users except for “admin” and any users in the “admin” group. By default, the Generic Users’ default permission is “No Access,” and no KVM port permissions are defined. Therefore, by default, any regular users that may be added cannot access any KVM ports. The KVM/net administrator can configure access to KVM ports for added regular users by:</p> <ul style="list-style-type: none"> • By selecting “[Generic Users]” and modifying the permissions - OR - • By configuring specific permissions for one or more individual users or groups (by selecting a single port or the “Multiple servers” option)

Table 7-18:User Access List KVM Port Permissions Configuration Screens

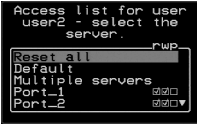
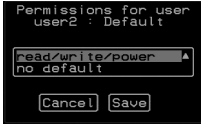
Screen	Description
<p>Access list for <i>username</i> - select the server</p> 	<p>The access list includes the “Reset all,” “Default,” “Multiple servers,” and “Exit” options along with each individual KVM ports.</p> <p>The “Default” option defines access permissions for all KVM ports, which apply unless the user has specific access permissions for any KVM ports.</p> <p>For a new user, because “Default Access,” is not defined, and also because no permissions are specified for that user’s access to any specific port, the Generic Users’ permissions apply.</p> <p>A series of three checkboxes appear to the right of each entry that has specific permissions (as defined in the following row). If a3 port has “No Access” defined, the checkboxes are empty. The headings for the checkboxes are: <i>rwp</i> for read, write, and power, and the boxes are checked appropriately when any of these permissions are defined. For example, in the screen to the left, the <i>r</i> and <i>w</i> boxes are checked next to “Port_1” and “Port_2,” which indicates that the user has read-write access to these ports.</p> <p>If “Reset all” is selected, the following confirmation screen appears.</p>



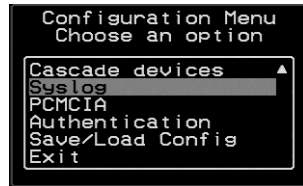
Table 7-18:User Access List KVM Port Permissions Configuration Screens

Screen	Description
Permissions for <i>username</i> : <i>port_number</i> or for <i>username</i> : followed by another Access list option, such as “Default” or “Multiple Servers”	The permissions from this menu can be configured to be “Default” permissions for all ports, applied to Multiple Servers, or applied to a selected port. Permissions menu options are “No Access,” Read-Only,” “Read Write,” “Read/Write/Power.” When “Default” is selected from the previous menu, the “Not Defined” menu option also appears. When any of the other options



Syslog Screens

You can select the Syslog option on the OSD Configuration Menu to specify the IP address for a syslog server.



Selecting the Configure>Syslog option brings up a Server screen for entering the IP address of a syslog server.

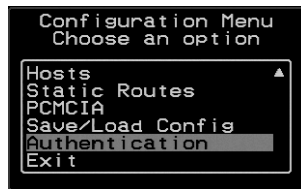


Figure 7-8: Syslog Configuration Server Screen

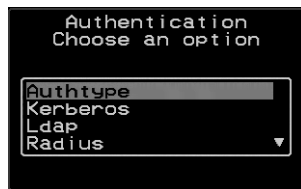
To complete the configuration of system logging, you must specify a facility number as shown in “Syslog Facility” on page 327.

Authentication Screens

You can select the Authentication option on the OSD Configuration Menu to configure an authentication type (AuthType) for logins to the KVM/net and to configure authentication servers for any type of logins: to the KVM/net or to KVM ports. See “Authentication” on page 44 for details about authentication on the KVM/net.



The Authentication menu appears as shown in the following figure.



Not all options are visible.

The following diagram lists the Authentication screens.

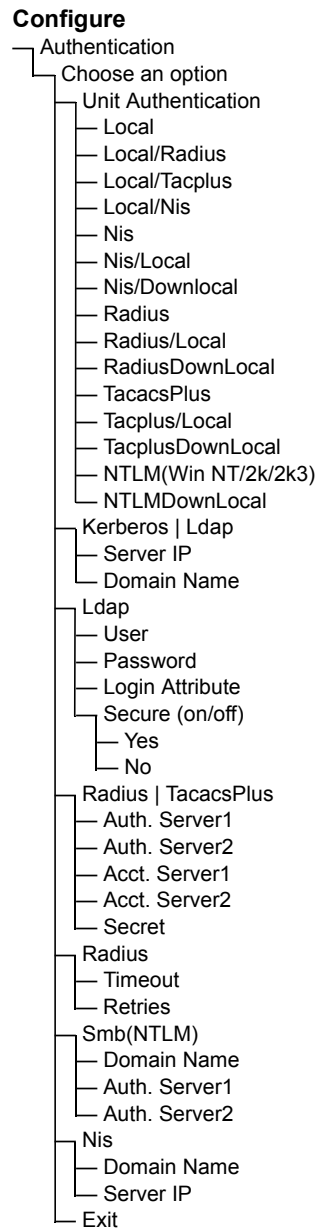
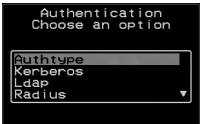
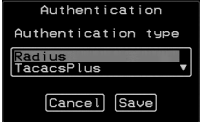


Figure 7-9: Authentication Options and Screens

On Screen Display

The following tables show the screens that appear when the “Authentication” option is selected from the Configure menu in the OSD. The first table shows the screen for choosing a KVM/net login authentication method.

Table 7-19:Authentication Configuration Screens for KVM/net Logins

Screen	Description
<p>Choose an option</p> 	<p>Choose either “Unit authentication” to select an Authentication method for KVM/net logins, or choose one of the Authentication methods listed on this screen to configure an authentication server: Kerberos, Ldap, Radius, TacacsPlus, Smb(NTLM), or Nis.</p>
<p>Authentication type</p> 	<p>Authentication method options for KVM/net logins. Default = “Local.” Other authorization type options are: Local/Radius, Local/Tacplus, Local/Nis, Nis, Nis/Local, Nis/Downlocal, Radius, Radium/Local, RadiusDownLocal, TacacsPlus, Tacplus/Local, TacplusDownLocal, NTLM(Win NT/2k/2k3), NTLMDownLocal</p>

The following table shows the common screens that appear when Kerberos or Ldap are selected to configure an authentication server.

Table 7-20:Common Configuration Screens for Kerberos and LDAP Authentication Servers

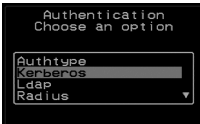
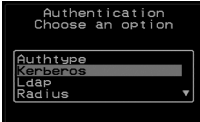


Screen	Description
<p>Ldap</p> 	<p>Choose Ldap to configure an LDAP authentication server.</p>
<p>Kerberos</p> 	<p>Choose Kerberos to configure a Kerberos authentication server.</p>

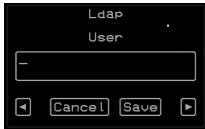


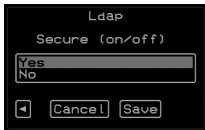
Table 7-20: Common Configuration Screens for Kerberos and LDAP Authentication Servers (Continued)

Screen	Description
Server IP 	IP address of the Kerberos or LDAP server.
Domain Name 	Domain name.

On Screen Display

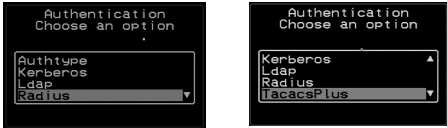
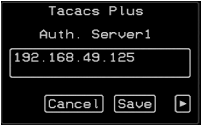

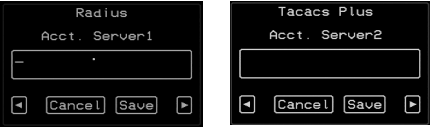


The following table shows the unique screens for configuring an LDAP server that appear in addition to the screens shown in Table 7-20, “Common Configuration Screens for Kerberos and LDAP Authentication Servers,” on page 7-376. The following table shows the configuration screens for the

Table 7-21: Unique LDAP Authentication Server Configuration Screens

Screen	Description
User 	The LDAP user name.
Password 	The LDAP password.
Login Attribute 	The login attribute.
Secure (on/off) 	Choices are “Yes” or “No.”

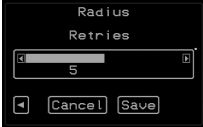
Radius and TACACS+ authentication servers. The following table shows the

Table 7-22: Configuration Screens for the Radius or TACACS+ Authentication Servers

Screen	Description
<p>Radius</p> <p>TacacsPlus</p> 	Choose Radius or TacacsPlus to configure a Radius or TACACS+ authentication server.
<p>Auth. Server1</p>  <p>Auth. Server2</p> 	IP addresses of one or two authentication servers. The second server is optional.
<p>Acct. Server1 and Acct. Server2</p> 	IP addresses of one or two optional accounting servers.
<p>Secret</p> 	Shared secret.
<p>Timeout</p> 	Appears only when Radius is selected. Timeout in seconds. The default is 3.

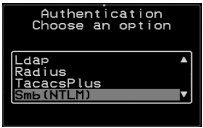

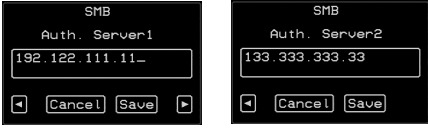
On Screen Display

Table 7-22: Configuration Screens for the Radius or TACACS+ Authentication Servers (Continued)

Screen	Description
Retries 	Appears only when Radius is selected. Number of retries. The default is 5.

Screens for configuring a Smb (NTLM) authentication server.

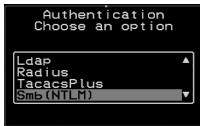
Table 7-23: Smb (NTLM) Configuration Screens

Screen	Description
Smb(NTLM) 	Choose Smb(NTLM) to configure an SMB (NTLM) authentication server.
Domain Name 	The domain name.
Auth. Server1 and Auth. Server2 	IP addresses for one or two SMB (NTLM) authentication servers. The second server IP is optional.

The following table shows the screens for configuring a NIS authentication server.

Table 7-24: NIS Configuration Screens

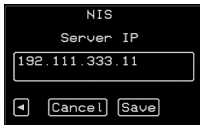
NIS	Choose the NIS authentication server
------------	--------------------------------------



Domain Name	Enter the Domain Name
--------------------	-----------------------

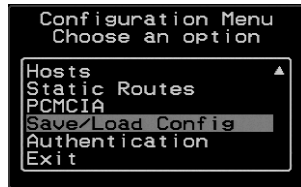


Server IP	IP address of the NIS server.
------------------	-------------------------------

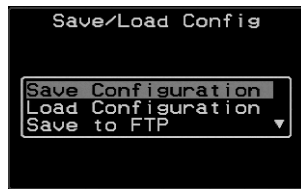


Save/Load Configuration Screens

You can use the Save/Load Config option on the OSD Configuration Menu to save any configuration changes you have made since the last save into a backup directory or onto an FTP server. You can also restore configuration file changes from a backup directory or FTP server to overwrite any configuration changes that were made since the last save.



The Save/Load Config screen appears as shown in the following figure. Not all options are visible.



The following diagram lists the Save/Load Configuration screens.

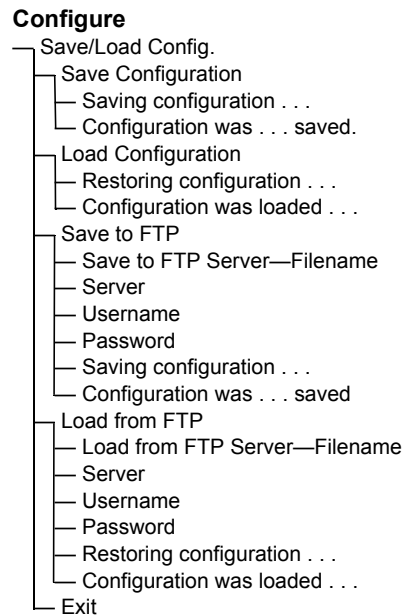


Figure 7-10: Save/Load Config Configuration Screens

The following table shows the screens that appear when the “Save/Load Configuration” option is selected from the Configure menu in the OSD.

Table 7-25: Save/Load Configuration Screens

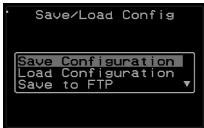
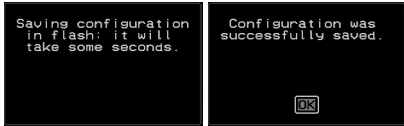
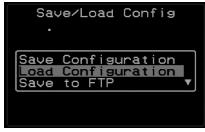

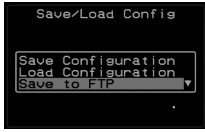
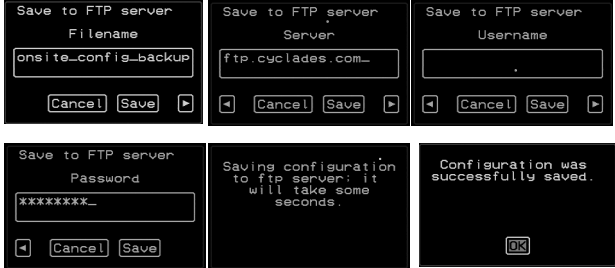
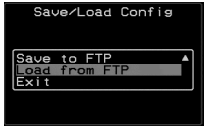

Screen	Description
<p>Save Configuration</p> 	<p>When “Save Configuration” is selected, the following two screens appear.</p> 

Table 7-25: Save/Load Configuration Screens (Continued)

Screen	Description
<p>Load Configuration</p> 	<p>When “Load Configuration” is selected, the following two screens appear.</p> 
<p>Save to FTP</p> 	<p>When “Save to FTP” is selected, the following five screens appear for you to enter the “Filename,” FTP “Server” name, FTP Login “Username” and “Password.” The last screens confirm the save to FTP succeeded.</p> 
<p>Load from FTP</p> 	<p>When “Load from FTP” is selected, the following four screens appear for you to enter the “Filename,” FTP “Server” name, FTP Login “Username” and “Password.”</p> 

System Info Menu

System Information window provides administrators detailed system information. The following table offers an example of the type of information you may see on the System Info window.

Table 7-26: System Information Example

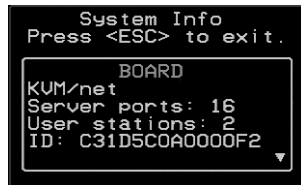
Information Type	Example
Board	KVM/net Server ports: 32 User stations: 2 ID: B7DA3C0A000011
Version	Firmware: 2.0 Orig. Boot: 2.0.7 Alt. Boot: no code SYS FPGA: 0x43 MUX FPGA: 0x5b
Memory	RAM: 128 Mbytes Flash: 16 Mbytes RAM usage: 17% RAMDISK usage: 100%
CPU	Clock: 48 MHz
Time	Mon Jul 19 2005 12:35:12 PDT up 10 min
User1 connection	Int. uC, V1.0.4
User2 connection	RP main, V1.0.4 RP local, V1.0.4

On Screen Display

▼ **To Access System Information**

1. On the Main Menu, select System Info.

The System Info window appears.



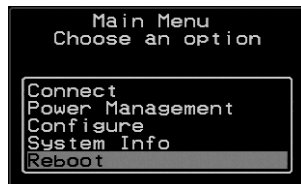
2. Use the up and down arrow keys to view the information.
3. To exit, press the escape key.

Reboot

You can reboot the KVM/net from the Main Menu of the OSD. This is particularly useful when operating through the RP.

▼ **To reboot the KVM/net**

1. Select Reboot from the Main Menu.



The following message appears.



2. Select Yes to reboot the KVM/net.

Controlling the OSD Through the AlterPath Remote Presence

While using the AlterPath Remote Presence (RP), an administrator has full access to the OSD menus, so all local administration tasks can be performed in an office or at any other location up to 500 feet away from the KVM/net. In addition, you do not need a dedicated monitor, keyboard, and mouse to use the RP; the RP box allows you to use the monitor, keyboard, and mouse of your regular workstation and use keyboard shortcuts to toggle between the view at your local work station and the view of the KVM/net.

See “Installing the AlterPath KVM Remote Presence” on page 118 for details on how to install an RP. No configuration is required to begin using the RP.

▼ **To Use to the AlterPath KVM RP to Access the KVM/net**

1. Connect the RP to the KVM/net using a CAT5 cable up to 500 feet long.

See “Installing the AlterPath KVM Remote Presence” on page 118 for detailed instructions and diagrams on how to connect the RP to the KVM/net and to your local work station.

2. Power on the RP.
3. Press the Select Local-Remote button on the front of the AlterPath KVM RP unit to switch the local video display from your local work station to the KVM/net OSD.

The OSD login screen appears.



4. Type your username followed by your password and press Enter.

The main menu of the KVM/net OSD appears. See “OSD Main Menu” on page 320 for a description of the OSD Main Menu items.

On Screen Display

5. Depending on your access privilege, perform one or more of the following actions:
 - If logged in as administrator, perform configuration tasks as described in “Configure Menu Overview” on page 323, “System Info Menu” on page 385, and “Reboot” on page 386.
 - If desired, connect to devices that are physically connected to the KVM/net.
See “Connection Menu” on page 321 for instructions.
 - If desired, power manage devices that are plugged into a configured AlterPath Power Management unit. (PM).
See “Power Management Menu” on page 322 for instructions.

▼ ***To Switch the RP Video Display from the OSD to the Local Computer***

Do one of the following:

- Press the following keyboard shortcut:
Scroll Lock Scroll Lock L
- Press the Select Local-Remote button on the RP front.
The green LED labelled Remote turns off, and the green LED labelled Local lights on.
By default the RP is set to beep when the monitor display switches from local to remote. See “To Turn the Beeper On or Off When Switching Between the Local and the Remote Work Stations” on page 389 for instructions on turning the beep on or off.

▼ ***To Switch the RP Video Display from the Local Computer to the OSD***

Do one of the following:

- Press the following keyboard shortcut:
Scroll Lock Scroll Lock R
- Press the Select Local-Remote button on the RP front.
The green LED labelled Local turns off, and the green LED labelled Remote lights on.

By default the RP is set to beep when the monitor display switches from local to remote. See “To Turn the Beeper On or Off When Switching Between the Local and the Remote Work Stations” on page 389 for instructions on turning the beep on or off.

▼ ***To Turn the Beeper On or Off When Switching Between the Local and the Remote Work Stations***

- Press the following keyboard shortcut:
Scroll Lock Scroll Lock B

On Screen Display

Appendix A

Troubleshooting

This chapter provides information and tasks related to troubleshooting the KVM/net in the following sections.

Replacing a Boot Image	Page 392
Downloading a New Software Version	Page 393
Changing the Boot Image	Page 394
To Boot in U-Boot Monitor Mode	Page 396
To Boot from an Alternate Image in U-Boot Monitor Mode	Page 396
To Boot in Single User Mode from U-Boot Monitor Mode	Page 397
To Replace a Boot Image From a Network Boot in U-Boot Monitor Mode	Page 397
To Restore the KVM/net Configuration to the Factory Default	Page 398

Replacing a Boot Image

How the KVM/net boots is introduced at a high level in “Boot Configuration” on page 244. The additional information in this section is to give an administrator with root access to the KVM/net enough understanding to be able to boot from an alternate image if the need arises and if the Web Manager is not available.

The KVM/net uses a U-Boot boot loader that resides in soldered flash memory and automatically runs at boot time. U-Boot boots the KVM/net from an image whose location is configurable. The image can reside either in removable flash memory on the KVM/net or on a boot server on the network. For more about U-Boot, go to: <http://sourceforge.net/projects/u-boot>.

By default, the KVM/net boots from the first partition.

- The KVM/net initially boots from a software image referred to as “image 1.”
- The first time you download and install a new software version from Cyclades, the new image is stored as “image 2” in the removable flash memory and the configuration is changed to boot the KVM/net from “image 2.”
- The second time you download a new software version, the latest image is stored as “image 1,” and the KVM/net configuration is changed to boot from “image 1.”
- Subsequent downloads are stored following the same pattern, alternating “image 1” with “image 2.”

Each image on the KVM/net’s removable flash has three separate file systems mounted on three Linux partitions. As shown in the following table, the first partition for each image is in VFAT (file allocation table) format, and it contains the Linux kernel. The second partition, in ext2 format, contains the root-mounted filesystem, and is read only. The third partition, in ext2 format, contains the configuration files and is read/write.

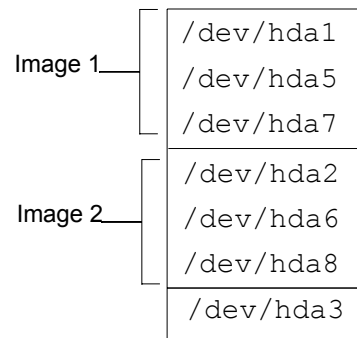
Table A-1: Boot Partitions, Formats, and Contents

Filesystem	Format	Contents
hda1	VFAT	Linux kernel for Image 1
hda2	VFAT	Linux kernel for Image 2

Table A-1: Boot Partitions, Formats, and Contents

Filesystem	Format	Contents
hda3	ex2	configuration backup
hda4	extended partition	
hda4	ext2	root filesystem for Image 1
hda6	ext2	root filesystem for Image 2
hda7	ext2	configuration for Image 1
hda8	ext2	configuration for Image 2

The following figure illustrates the partitions where Image 1 and Image 2 are stored.



Downloading a New Software Version

You can download a new software version in the following ways:

- Use the Web Manager Firmware Upgrade form to download the image from an FTP server

When the image is downloaded by FTP, a script (`saveimage`) automatically extracts the filesystem from the image, mounts it, and copies the files to the removable flash. If a current version of the image is being run from one of the three-partitions sets, the downloaded image is stored in

the other set of partitions. The environment variable `currentimage` is changed so that the system boots from the new image.

- Do a network boot from the new image and then save it onto the removable flash

The monitor command `net_boot` boots the image from the TFTP server specified in the environment variables. After the image is downloaded by network boot, the root filesystem is in the RAMDISK, and the image can run even if there is no removable flash card is inserted.

From the command line, you can run the `create_cf` script with the `--doformat` option to automatically save the image in removable flash. The script erases everything in the flash, partitions the flash, if necessary, formats the partitions, and copies the files currently in the RAMDISK into the corresponding image partitions. If the flash is already partitioned, you can choose where the image is saved using the option `--imageN`.

Changing the Boot Image

If, for any reason, you want to change to another image from the current one, if you have access to the Web Manager, you can use the Configuration > System > Boot Configuration form in Expert mode to select the other image, and then use the reboot button on the Management > Reboot form in Expert mode to reboot the KVM/net.

You can use the Linux `bootconf` options if you do not have access to the Web Manager. See “To Boot from an Alternate Image With `bootconf`” on page 394.

You can also boot in U-Boot monitor mode and use the available boot commands. See “To Boot in U-Boot Monitor Mode” on page 396.

▼ To Boot from an Alternate Image With `bootconf`

1. Connect to the KVM/net from a terminal connected to the console port or create a `telnet` or `ssh` connection, and log in as root.
2. Enter the `bootconf` command.

```
# bootconf
```

The `bootconf` application prompts you for values to accept or change.

3. Press “Enter” to accept the current values as prompted until the “Image names” and the prompt shown in the following screen example appear.

```
Image names:
image1:zvmppcons.v100
image2:zvmppcons.v102

Current image (image(1) or image(2)) [1] :
```

4. Enter the number of the alternate image to boot from.

The following screen example shows the number 2 entered to configure booting from image 2.

```
Current image (image(1) or image(2)) [1] :2
```

5. Enter **Y** when prompted: “Do you confirm these changes in flash.”

```
Do you confirm these changes in flash ( (Y)es, (N)o (Q)uit ) [N] :Y
```

6. Restart the KVM/net.

```
[root@ons /]# reboot
```

Changing the Boot Image in U-Boot Monitor Mode

You can access U-Boot monitor mode in one of the following two ways:

- During boot, when the “Hit any key to stop autoboot” prompt appears, pressing any key before the timer expires brings the KVM/net to monitor mode.
- If boot fails, the KVM/net automatically enters monitor mode.

The U-Boot `hw_boot` command boots from either the first or second image according to the value of the “currentimage” environment variable, which can be either 1 or 2. You can use the following procedures to specify another image.

"To Boot in U-Boot Monitor Mode"	Page 396
To Boot from an Alternate Image in U-Boot Monitor Mode	Page 396

To Boot from an Alternate Image With bootconf	Page 394
---	----------

To Boot in Single User Mode from U-Boot Monitor Mode	Page 397
--	----------

▼ **To Boot in U-Boot Monitor Mode**

1. Open a terminal connection to the console port, and log in as root.
2. Enter the `reboot` command.

```
# reboot
```

3. During boot, when the “Hit any key to stop autoboot” prompt appears, press any key before the time elapses to stop the boot.
4. The U-Boot monitor prompt appears:

```
=>
```

5. Enter `help` to see a list of supported commands.

```
=> help
```

▼ **To Boot from an Alternate Image in U-Boot Monitor Mode**

1. Go to U-Boot monitor mode.
See "To Boot in U-Boot Monitor Mode" if needed.
2. Set the current image environment variable to the number of the image you want to boot.

```
=> setenv currentimage N
```

For example, to boot from image 2 enter the number 2, as shown in the following screen example.

```
=> setenv currentimage 2
```


3. Enter the boot command.

```
=> hw_boot
```

▼ **To Boot in Single User Mode from U-Boot Monitor Mode**

1. See “To Boot in U-Boot Monitor Mode” on page 396 if needed.
2. Boot by entering `hw_boot` followed by `single`, as shown in the following screen example.

```
=> hw_boot single
```

▼ **To Replace a Boot Image From a Network Boot in U-Boot Monitor Mode**

After performing a network boot, you can use the `create_cf` command at any time to save the files in the removable flash. The only changes you should make before running `create_cf` are configuration file changes.

1. Log in as root.
2. Set the “bootfile,” “serverip,” and “ipaddr” environment variables using the boot filename, the boot server’s IP address, and the IP address of the KVM/net to use for network booting.

The format of the boot filename is: `zmpcons.vversion_number`, for example: `zmpcons.v120`.

```
=> setenv ipaddr KVM/net's_IP_address
=> setenv serverip boot_server's_IP_address
=> setenv bootfile boot_file's_name
```

3. Check that the environment variables are set properly with the `showenv` command.

```
=> printenv
```

Troubleshooting

4. Enter the `net_boot` command.

```
=> net_boot
```

5. Log in as root after boot completes.
6. Run the `create_cf` command with the `--doformat` argument.

```
[root@ons root]# create_cf --doformat
```

7. Configure the KVM/net to boot from flash.
8. Reboot.

▼ **To Restore the KVM/net Configuration to the Factory Default**

This procedure assumes that the `saveconf` command has been previously run to save the configuration.

- While logged in as root through the console, via `telnet`, or via any `ssh` session, enter the `restoreconf` command with the `factory_default` option.

```
[root@ KVM/net root]# restoreconf factory_default
```

```
restoreconf:
Usage:
Restore from flash:          restoreconf
Restore from factory default: restoreconf factory_default
Restore from storage device: restoreconf sd
Restore from local file:    restoreconf local <FILE>
Restore from FTP server:    restoreconf ftp <FILE>
<FTP_SERVER> <USER> <PASSWORD>
Restore from TFTP server:    restoreconf tftp <FILE>
<TFTP_SERVER>
Restore from SSH server:    restoreconf ssh <FILE>
<SSH_SERVER> <USER>
```

Glossary

3DES	Tripple Data Encryption Standard, an encrypting algorithm (cipher) that processes each data block three times, using a unique key each time. 3DES is much more difficult to break than straight DES. Because it is the most secure of the DES combinations, 3DES is also slower in performance.
authentication	The process by which a user's identity is checked within the network to ensure that the user has access to the requested resources.
basic in/out system (BIOS)	Chips on the motherboard of a computer contain read only memory instructions that are used to start up a computer. The operating system of a PC also makes use of BIOS instructions and settings to access hardware components such as a disk drive. Some BIOS/CMOS settings can be set to scan for viruses, causing problems for some installation programs.
baud rate	The baud rate is a measure of the number of symbols (characters) transmitted per unit of time. Each symbol will normally consist of a number of bits, so the baud rate will only be the same as the bit rate when there is one bit per symbol. The term originated as a measure for the transmission of telegraph characters. It has little application today except in terms of modem operation. It is recommended that all data rates are referred to in bps, rather than baud (which is easy to misunderstand). Additionally, baud rate cannot be equated to bandwidth unless the number of bits per symbol is known.
BogoMips	A measurement of processor speed made by the Linux kernel when it boots, to calibrate an internal busy-loop.
boot	To start a computer so that it is ready to run programs for the user. A PC can be booted either by turning its power on, (Cold Boot) or by pressing Ctrl+Alt+Del (Warm Boot).

Glossary

bootp	Bootstrap Protocol. A TCP/IP protocol allowing a BOOTP server node to allocate IP addresses to diskless workstations at startup.
CAT5	Category 5. A cabling standard for use on networks at speeds up to 100 Mbits including FDDI and 100base-T. The 5 refers to the number of turns per inch with which the cable is constructed.
console	Terminal used to configure network devices at boot (start-up) time. Also used to refer to the keyboard, video and mouse user interface to a server.
checksum	A computed value which depends on the contents of a block of data and which is transmitted or stored along with the data in order to detect corruption of the data. The receiving system recomputes the checksum based upon the received data and compares this value with the one sent with the data. If the two values are the same, the receiver has some confidence that the data was received correctly.
DHCP	<p>Dynamic Host Configuration Protocol. A protocol for automatic TCP/IP configuration that provides static and dynamic address allocation and management.</p> <p>DHCP enables individual computers on an IP network to extract their configurations from a server (the 'DHCP server') or servers, in particular, servers that have no exact information about the individual computers until they request the information. The overall purpose of this is to reduce the work necessary to administer a large IP network. The most significant piece of information distributed in this manner is the IP address.</p>
escape sequence	<p>A sequence of special characters that sends a command to a device or program. Typically, an escape sequence begins with an escape character, but this is not universally true.</p> <p>An escape sequence is commonly used when the computer and the peripheral have only a single channel in which to send information back and forth. If the device in question is "dumb" and can only do one thing with the information being sent to it (for instance, print it) then there is no need for an escape sequence. However most devices have more than one</p>

capability, and thus need some way to tell data from commands.

Ethernet

A LAN cable-and-access protocol that uses twisted-pair or coaxial cables and CSMA/CD (Carrier Sense Multiple Access with Collision Detection), a method for sharing devices over a common medium. Ethernet runs at 10 Mbps; Fast Ethernet runs at 100 Mbps. Ethernet is the most common type of LAN.

Flash

Flash refers to a type of memory that can be erased and reprogrammed in units of memory known as blocks rather than one byte at a time; thus, making updating to memory easier.

flow control

A method of controlling the amount of data that two devices exchange. In data communications, flow control prevents one modem from "flooding" the other with data. If data comes in faster than it can be processed, the receiving side stores the data in a buffer. When the buffer is nearly full, the receiving side signals the sending side to stop until the buffer has space again. Between hardware (such as your modem and your computer), hardware flow control is used; between modems, software flow control is used.

Hot-Swap

Ability to remove and add hardware to a computer system without powering off the system.

IP address

A 32-bit address assigned to hosts using TCP/IP. It belongs to one of five classes (A-E) and is expressed as 4 octets separated by periods formatted as dotted decimals. Each address has a network number, an optional sub network number and a host number. The first two numbers are used for routing, while the host number addresses an individual host within the network or sub network. A subnet mask is used to extract network and sub network information from the IP address.

IP packet filtering

This is a set of facilities in network equipment that allows the filtering of data packets based on source/destination addresses, protocol, TCP port number and other parameters. Packet filtering is one of the main functions of a firewall.

Glossary

IPsec	Short for <i>IP Security Protocol</i> , IPsec is an extended IP protocol that provides encrypted security services. These services enable authentication, as well as access and trustworthiness control. IPsec provides similar services as SSL, but it works on a network layer. Through IPsec you can create encrypted tunnels (VPN) or encrypt traffic between two hosts.
Kerberos	Kerberos was created by MIT as a solution to network security problems. The Kerberos protocol uses strong cryptography so that a client can prove its identity to a server (and vice versa) across an insecure network connection. After a client and server has used Kerberos to prove their identity, they can also encrypt all of their communications to assure privacy and data integrity as they go about their business.
KVM	Keyboard, video and mouse interface to a server.
LDAP	Lightweight Directory Access Protocol. A software protocol for enabling anyone to locate organizations, individuals, and other resources such as files and devices in a network, whether on the Internet or on a corporate intranet. LDAP is a "lightweight" (smaller amount of code) version of DAP (Directory Access Protocol), which is part of X.500, a standard for directory services in a network.
MAC	Medium Access Control. Internationally unique hardware identification address that is assigned to the NIC (Network Interface Card) which interfaces the node to the LAN.
network mask	<p>A number used by software to separate the local subnet address from the rest of a given Internet protocol address</p> <p>Network masks divide IP addresses into two parts (network address and address of a particular host within the network). Mask have the same form as IP addresses (i.e. 255.255.255.0), however, its value is needed to be understood as a 32-bit number with certain number of ones on the left end and zeros as the rest. The mask cannot have an arbitrary value. The primary function of a subnet mask is to define the number of IP hosts that participate in an IP subnet. Computers in the same IP subnet should not require a router for network communication.</p>

NTP	<i>Network Time Protocol.</i> A standard for synchronizing your system clock with the "true time", defined as the average of many high-accuracy clocks around the world.
OSD	On-Screen Display.
packet	A packet is a basic communication data unit used when transmitting information from one computer to another. The maximum length of a packet depends on the communication medium. As an example, in Ethernet networks the maximum length is 1500 bytes. A data packet can be divided into two parts: the header part and the data part. The header contains information needed for communication between nodes; the data is the body of the packet that is ultimately received by the application.
parity	<p>In serial communications, the parity bit is used in a simple error detection algorithm. As a stream of data bits is formed, an extra bit, called the parity bit, is added. This bit is set on (1) or off (0), depending on the serial communications parameters set in the UART chip.</p> <p>The following lists the available parity parameters and their meanings:</p> <p>Odd – Parity bit set so that there is an odd number of 1 bits</p> <p>Even – Parity bit set so that there is an even number of 1 bits</p> <p>None – Parity bit is ignored, value is indeterminate</p>
PCMCIA	Personal Computer Memory Card International Association – An organization that supports standards for a compact hardware interface that accepts a variety of devices such as modems, storage, and other devices.
port	A port is a 16-bit number (the allowed range being 1 through 65535) used by the TCP and UDP protocols at the transport layer. Ports are used to address applications (services) that run on a computer. If there was only a single network application running on the computer, there would be no need for port numbers and the IP address only would suffice for addressing services. However, several applications may run at once on a particular computer and we need to differentiate among them. This is what port numbers are used for. Thus, a

Glossary

port number may be seen as an address of an application within the computer.

PPP

Point-to-Point Protocol. This protocol is a way to connect your computer to the Internet over telephone lines. PPP is replacing an older protocol, SLIP, as it is more stable and has more error-checking features.

PPP has been a widely-used Internet standard for sending datagrams over a communications link. The PPP standard is described in RFC 1661 by the Point-to-Point Working Group of the Internet Engineering Task Force (IETF). PPP is commonly used when remote computers call an Internet service provider (ISP) or a corporate server that is configured to receive incoming calls.

RADIUS

Remote Authentication Dial-In User Service) is a client/server protocol and software that enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service. RADIUS allows a company to maintain user profiles in a central database that all remote servers can share.

RC4

Rivest Cipher four, an encryption method using variable length secret key streams. RC4 is an alternate to DES and is approximately ten times as fast as DES; however, it is less secure.

SMTP

Simple Mail Transfer Protocol. Specifies the format of messages that an SMTP client on one computer can use to send electronic mail to an SMTP server on another computer.

SNMP

Short for *Simple Network Management Protocol*, a set of protocols for managing complex networks. The first versions of SNMP were developed in the early 80s. SNMP works by sending messages, called protocol data units (PDUs), to different parts of a network.

SNMP-compliant devices, called agents, store data about themselves in Management Information Bases (MIBs) and return this data to the SNMP requesters.

(Source: Webopedia)

SNMP Traps	<p>Notifications or Event Reports are occurrences of Events in a Managed system, sent to a list of managers configured to receive Events for that managed system. These Event Reports are called Traps in SNMP. The Traps provide the value of one or more instances of management information.</p> <p>Any SNMP enabled Device generates Fault Reports (Traps) that are defined in the MIB (which the SNMP Agent has implemented).</p> <p>The Trap Definition vary with the SNMP Version (which defines the messaging format), but the information contained in these are essentially identical. The major difference between the two message formats is in identifying the events.</p>
SSH	<p>Secure Shell. A protocol which permits secure remote access over a network from one computer to another. SSH negotiates and establishes an encrypted connection between an SSH client and an SSH server.</p>
Stop Bit	<p>A bit which signals the end of a unit of transmission on a serial line. A stop bit may be transmitted after the end of each byte or character.</p>
Subnet Mask	<p>A bit mask used to select bits from an Internet address for subnet addressing. Also known as Address Mask.</p>
TACACS	<p>Terminal Access Controller Access Control System.</p> <p>Authentication protocol, developed by the DDN community, that provides remote access authentication and related services, such as event logging. User passwords are administered in a central database rather than in individual routers, providing an easily scalable network security solution.</p>
TACACS+	<p>Terminal Access Controller Access Control System Plus. A protocol that provides remote access authentication, authorization, and related accounting and logging services, used by Cisco Systems.</p>
Telnet	<p>A terminal emulation program for TCP/IP networks such as the Internet. The Telnet program runs on your computer and connects your PC to a server on the network. You can then enter commands through the Telnet program and they will be</p>

Glossary

executed as if you were entering them directly on the server console.

TFTP

Trivial File Transfer Protocol. A simple network application based on User Datagram Protocol (UDP). It is used to transfer files from one computer to another.

TTY

1. In Unix, refers to any terminal; sometimes used to refer to the particular terminal controlling a given job (it is also the name of a Unix command which outputs the name of the current controlling terminal). 2. Also in Unix, any serial port, whether or not the device connected to it is a terminal; so called because under Unix such devices have names of the form **tty**.

UDP

User Datagram Protocol uses a special type of packet called a datagram. Datagrams do not require a response; they are one way only (connectionless). Datagrams are usually used for streaming media because an occasional packet loss will not affect the final product of the transmission.

VPN

Virtual Private Networking allows local area networks to communicate across wide area networks, typically over an encrypted channel. See also: **IPsec**.

Watchdog timer

Mechanism to detect hardware and operating system failures.

Index

Numerics

3DES 193, 358
56K 338

A

access 153
 in-band server 4
 user 68
 user and group 189
access connected devices 294
Access Control 366
Access list for username - select the server 402
access system information, to 419
access to
 a user or group, to assign KVM port 190
 connected devices, tasks related to 40
 KVM ports, enabling direct 166
 KVM ports, to enable direct 166
 ports 40
 RDP servers 208
 Web Manager 100
 Web Manager, default IP address 100
 Web Manager, dynamic IP address 101
Access window 6, 310, 316
Access window tab 312
accessing
 cascaded ports 30
 in-band servers 298
 KVM RP 130
 KVM servers 299
 Acct. Server1 and Acct. Server2 412
 ACK 227
 ACK Flag 377
 Active 388
 active sessions 282
 killing 283
 viewing information on 282
 activity LEDs 17
 activity LEDs, front panel 19
adding
 a group 188
 chain 232
 chain for IP filtering 234
 KVM Expander 67
 packet filtering rule 234
 RDP server 209
 rule for IP filtering 236
 secondary KVM 177
 syslog server 150
 user 145, 186
admin, Web Manager 138
admin's default password, changing 98
administering users of connected servers 40
administration options 25
administrative modes 141
administrators' Windows, common features of 136
alarms and logging 56
alarms and syslog 53
alarms and syslog, configuring 160
Alias 380
alias for a KVM port, specifying 184
AlterPath KVM Expander, installing 118

Index

- AlterPath KVM RP 69
 - AlterPath KVM RP, controlling the OSD through the 420
 - AlterPath KVM RP, installing the 128
 - AlterPath KVM/net, shipping box contents 73
 - AlterPath PM, upgrading 161
 - AlterPath PMs, connecting 116
 - AlterPath RP 420
 - AlterPath Viewer and Access window tab, to connect to another port using the current 312
 - AlterPath Viewer options, setting 337
 - AlterPath Viewer settings 335
 - AlterPath Viewer, to connect to the previous or next authorized port without opening a new 314
 - among authentication methods, choosing 50
 - another port using the current AlterPath Viewer and Access window tab, to connect to 312
 - Any 227
 - Auth. Server1 and Auth. Server2 413
 - authentication 50
 - authentication for KVM port logins 168
 - authentication method 196, 244
 - configuring an 195
 - KVM ports 168
 - KVM ports 197
 - authentication methods
 - choosing among 50
 - tools for specifying 52
 - Authentication Protocol 244
 - Authentication Required, PPP configuration 256
 - authentication screens 407
 - authentication server
 - Kerberos 199
 - LDAP 201
 - NIS 204
 - Radius 205
 - SMB(NTLM) 203
 - TACACS+ 206
 - authentication servers 198
 - Authentication Type 357
 - Authentication type 409
 - Auto 338
 - Auto Sync Mouse 336
 - AUX 1 port for use with a PM, to configure the 254
 - AUX 1 port, to connect a PM to the 116
 - AUX 2 port for use with an external modem, to configure the 254
 - AUX port - PPP 391
 - Baud Rate 391
 - Data Size 392
 - Flow Control 391
 - Local IP 392
 - Parity 392
 - Remote IP 392
 - Stop Bits 392
 - AUX port, connecting an external modem 114
 - AUX ports
 - configuring with OSD 390
 - configuring with Web Manager 253
 - description 16
 - AUX ports - Protocol 391
 - AUX ports screens, OSD 390
- ## B
- back KVM RP 69
 - back KVM/net 12
 - back up configuration data 273
 - Backspace 348
 - backup configuration 271
 - Baud Rate, PPP configuration 255
 - beep, KVM RP 422

- beeper on AlterPath KVM RP 422
- Board 418
- Boot Action 371
- Boot Action, Local 244
- boot configuration 259
- Boot File Name 261
- boot image 428
- boot image, changing the 426
- boot, to configure 262
- bootconf 426
- box contents KVM Expander, shipping 119
- box contents KVM RP, shipping 129
- box contents KVM/net, shipping 73
- brackets, mounting 74, 120
- brightness, adjusting screen 314, 315, 329
- buffering, data 53

C

- cabling
 - white paper and ordering 74, 120
- callback 406
- callback phone 406
- card slots, PCMCIA 5
- card, PCMCIA 17
 - configuring a modem 219
 - eject PCMCIA 222
 - installing 113
 - removing 114
 - to configuring a modem 219
- Cascade Device Add Device 394
- Cascade Device Delete Device 395
- Cascade deviceAdd device Select Model 395
- Cascade deviceChoose an option 394
- cascade devices 393
- cascaded devices 29
 - accessing ports on 30
 - adding 177
 - configuring 176

- connecting 125
- deleting configuration of 180
- editing configuration of 178
- KVM Expander 64
- reading the port numbers of 306
- chain
 - adding 232, 234
 - editing 232, 236
- Chain - CHAIN_NAME 374
- Chain - chain_name 374
- Chain Name 374
- changing default passwords 99
- check boxes, inverted 225
- Choose an option 398, 399, 409
- closing a KVM connection 332
- closing a local KVM connection 332
- code, upgrading the KVM Expander
 - microcontroller 67
- Comments field 187
- Community 246, 247
- computers to KVM ports, to connect 80
- computers to the KVM ports, connecting 78
- configuration 159, 163
 - back up or retrieve 273
 - backup 271
 - basic network 84
 - boot 259
 - cascaded KVM unit 178, 180
 - changes, to save 140
 - direct connection for network 82
 - factory default 430
 - firewall 231
 - network 360
 - tasks 104
 - Web Manager 97
- configuration screen series, understanding
 - OSD 356
- configuration screens
 - Date/time 383
 - General 357

Index

- Hosts 379
- IP Filtering 372
- Network 361
- Save/load 415
- SNMP 364
- Static Routes 380
- VPN 368
- Configure 351
- configure menu overview 353
- configuring
 - authentication method 195
 - authentication method for logins through KVM ports 197
 - authentication method, KVM/net logins 196
 - authentication servers 198
 - AUX 1 port 254
 - AUX 2 port 254
 - basic networking
 - OSD 88
 - wiz command 85
 - boot 262
 - cascaded KVM units 176
 - creation of alarms and syslog files for IPDUs 160
 - encryption on port connections 194
 - host settings 215
 - hosts 249
 - in-band (RDP) servers 207
 - IP user (KVM over IP) sessions 173
 - KVM port for power management 175, 182
 - local User 1 and User 2 sessions 172
 - logging and alarms 56
 - modem (PCMCIA) card 219
 - modem card 219
 - network parameters, OSD 92
 - network parameters, wiz command 86
 - NIS authentication server 204
 - power management 47
 - PPP connection on a remote computer 343
 - SMB(NTLM) authentication server 203
 - SNMP 245
 - syslogging 218
 - users to manage specific power outlets 158
 - VPN 242
- conflicting mouse settings, avoiding 105
- conflicts, avoiding Internet Explorer 108
- conflicts, preventing mouse 105, 106, 107
- Connect 350
- Connect read only 333
- Connect read write 334
- Connect to Server drop-down list 305
- Connect to Server form 308
- connected devices
 - accessing 40
 - authentication 198
 - power on 83
 - powering on 83, 124
 - who can access 294
- connected port information, viewing 312, 327
- connected servers, administering users of 40
- connecting
 - AlterPath PMs 116
 - another port 312
 - cascaded KVM units 125
 - computers to KVM ports 80
 - computers to the KVM ports 78
 - Connect to Server drop-down list 305
 - external modem 114
 - external modem to an AUX port 114
 - KVM Expander 127
 - KVM port through the login screen 306
 - KVM RP to the local work station 131
 - multiple PMs 117
 - PM to the AUX 1 port 116
 - servers with the OSD 322

- servers with the Web Manager 304
 - servers, preparing for 79
- connecting to
 - servers 153
- connection
 - closing a local KVM 332
 - closing KVM 332
 - direct 82
 - Ethernet 77
 - PPP 345
 - quitting the port 317
 - resuming port 317
 - sharing server 319
 - sharing server 317
 - terminal emulator dial up 345
- connection menu 338, 351
- connection menu, OSD 323
- Connection Name 369
- connection type 38
- connections
 - Access window 6
 - daemons used for incoming 224
 - encryption on port 194
 - modem 342
 - prerequisites for in-band 298
 - prerequisites for KVM 299
 - sharing KVM port 333
 - simultaneous server 23
 - through the OSD, controlling local KVM
 - port 324
 - viewing in-band 298
 - viewing KVM 296
- Connector Name 243
- console
 - port, connection 82
 - port, logging in through the 85
 - port, changing the password through the
 - 85
- contrast, adjusting screen 314
- CPU 418

- Cyclades Web Manager 26
- cycle 313, 328
- Cycle Time 171
- Cycling 386
- cycling 313, 328

D

- daemons 224
- daisy chaing power 124
- data buffering 53
- Data Size, PPP configuration 255
- data, backing up configuration 273
- date and time
 - manual setting 257
 - NTP 258
 - OSD 95
- date/time configuration screens 383
- default
 - IP address 100
 - password, changing admin's 98
 - passwords, changing 98, 99
 - restore factory 430
- deleting
 - cascaded KVM unit 180
 - in-band (RDP) server 212
 - syslog server 150
 - user 147
 - user or group 187
- description 2
- Destination IP 375
- Destination IP field 226
- Destination Mask 376
- Destination Port 227, 376
- Device 382
- devices
 - accessing connected 40
 - accessing ports on cascaded KVM 30
 - cascade 393

Index

- cascaded 29
- daisy chained on KVM Expander 124
- power on connected 83
- power on KVM-connected 124
- powering on connected 83, 124
- preparing to connect 79
- reading port numbers of cascaded 306
- who can access connected 294
- DHCP, configuring 362
- DHCP, description 56
- dial in 346
- dial up connection 345
- Direct Access 358
- direct access to KVM ports, enabling 166
- direct connection 82, 100
- disabling KVM ports 184
- DNS Server 363
- document
 - audience xxxi
 - CD xxxiii
 - downloads xxxiii
 - organization xxxii
 - related documentation xxxiii
- Domain 363
- Domain Name 410, 413, 414
- download microcode 279
- downloading
 - documents xxxiii
- downloading new software 425
- DSL 338
- dynamic IP address 101
- E**
- echo-reply 241
- editing
 - chain 232
 - chain for IP filtering 236
 - configuration of a cascaded KVM unit 178
 - rule for IP filtering 233
 - rule options 225
- ejecting PCMCIA cards 222
- enabling
 - access to Web Manager 100
 - direct access to KVM ports 166
 - KVM ports 184
- Encrypt Everything 338
- Encrypt Keyboard and Mouse 338
- encryption 49
- encryption on port connections, configuring 194
- Encryption Type 338
- End 348
- Enter 348
- Enter the group name 399
- Enter the password 398
- Enter the username 400
- Esc 348
- Escape Sequence 358
- escape sequence
 - conventions for xxxv
- Ethernet connection, making an 77
- Exit 351
- Expander
 - cascading 64
 - connecting 127

- features 61
- installing 118
- KVM 60
- LEDs 64
- list of cascaded devices 67
- microcontroller code, upgrading 67
- models and components 62
- mounting 121
- ports 63
- power outlets 64, 124
- powering on 124
- setting up 121
- shipping box contents 119
- enabling direct access to KVM ports 166
- Expert mode 151
- Expert mode, overview 152
- external modem
 - configuring 254
 - connecting 114

F

- facility numbers
 - example 55
 - syslog messages 55
- factory default, restoring configuration to 430
- Fast Ethernet 261
- Fast Ethernet Max Interrupt Events 261
- features of administrators' Windows,
 - common 136
- features, KVM Expander 61
- Field Adjacent to Go to 252
- fields
 - ICMP protocol 228
 - numeric protocol 227
 - TCP protocol 227
 - UDP protocol 228
- Filter Table 374

- filtering
 - chain for IP 234, 236
 - configuration screens, IP 372
 - IP 224
 - KVM port message 218
 - packet 44
 - packet rule adding 234
 - rule for IP 233, 236
- FIN 227
- FIN Flag 377
- firewall configuration procedures 231
- firmware upgrade 274, 277
 - AlterPath PM 161
 - Cyclades pathname for 276
- Flow Control, PPP configuration 255
- Force Screen Auto Alignment 336
- Force Screen Refresh 336
- forms
 - conventions for showing how to navigate to xxxv
- FORWARD packet 224
- Fragments 230, 378
- FTP server, download microcode 279

G

- Gateway 363, 382
- Gateway or Device 382
- general 164, 165, 263
- general configuration screens 357
- general information 263
- GMT 258
- Go to 252
- Go to a specific window, as in
 - Go to Configure>Users and Groups.” 349
- Graph BG Color 269
- Graph Type 269
- Grey Scale 339

Index

Grid Line Color 269

Group field 186

groups

- adding 188

- assign KVM port access to 189, 190

- deleting 187

- modifying 188

- screens 396

guidelines for using the KVM/net 9

H

hierarchy, KVM port permissions 33

High Color 339

Home 348

Host IP 252

Host or Net Route 382

host settings 214

host settings, configuring 215

host tables 249

Hostname 363

hosts configuration screens 379

hosts, configuring 249

hot keys

- conventions for xxxv

- for emulating sun keyboard keys 326

- for local station 325

- redefining KVM connection 42

- redefining sun keyboard equivalent 42

- summary of tasks for redefining 43

I

ICMP protocol fields 228

ICMP Type 378

icmp-host-prohibited 241

icmp-host-unreachable 241

icmp-net-prohibited 241

icmp-net-unreachable 241

icmp-port-unreachable 241

icmp-proto-unreachable 241

ID, Local 244

ID, Remote 244

idle timeout

- configuring 170, 385

- resuming port connection after 317

IE security settings, modifying 108

in-band access to RDP servers, prerequisites for 208

in-band connections, prerequisites for accessing servers with 298

in-band connections, viewing 298

in-band server

- access, description 4

- adding 209

- configuring 207

- deleting 212

- modifying 209

info menu, system 418

info, view IPDUs 157

information

- access system 419

- obtaining more 137

- view active sessions 282

- view and reset IPDU 157

- view connected port 312, 327

- viewing system 263

information displayed on the Access window, to refresh the 316

Input Interface 230, 377

input interface, output interface, and fragments 229

INPUT packet 224

install a PCMCIA card in the front card slot, to 113

installation, preconfiguring for remote 103

installing AlterPath KVM Expander 118

installing AlterPath KVM RP 128

- installing PCMCIA cards in the front card slots 113
- Internet Explorer conflicts, avoiding 108
- Inverted check boxes 225
- IP 380
- IP Address 362
- IP address
 - default 100
 - dynamic 101
- IP Address, Local 244
- IP Address, Remote 244
- IP filtering 224
 - add a chain for 234
 - add a rule for 236
 - configuration screens 372
 - edit a chain for 236
 - edit a rule for 233
- IP Local 406
- IP Options 240
- IP Remote 406
- IP Security Level 358
- IP user (KVM over IP) sessions, to configure 173
- IP user sessions, configuring 173
- IP users, local user and 169
- IPDU information, to view and reset 157
- IPDU power management 154
- IPDU power management forms, controlling power through the Web Manager 48
- IPDUs info, view 157
- IPDUs, alarms and syslog 160

K

- Kerberos 198, 409
- Kerberos authentication server, configuring 199
- keyboard
 - and mouse, resetting the 330

- and mouse, to reset the 330
- equivalent hot keys, redefining sun 42
- keys, hot keys for emulating sun 326
- shortcuts (hot keys), redefining 42
- shortcuts (hot keys), redefining KVM connection 166
- shortcuts, to redefine KVM session 167
- Keyboard Type 171, 386
- keys
 - basic navigation 348
 - conventions for hot keys, escape keys, and keyboard shortcuts xxxv
 - hot keys for emulating sun keyboard 326
 - redefining KVM connection hot 42
 - redefining sun keyboard equivalent hot 42
 - summary of tasks for redefining hot 43
- keys for
 - local, hot 325
- Kill other session 334
- killing active session 283
- KVM 164
- KVM connections
 - closing 332
 - closing local 332
 - hot keys, redefining 42
 - keyboard shortcuts, redefining 166
 - prerequisites 299
 - viewing 296
- KVM devices
 - accessing ports on cascaded 30
 - port numbers of cascaded 306
- KVM Expander 60
 - cascading a 64
 - connect to master 127
 - features 61
 - installing 118
 - LEDs 64
 - master device list 67
 - microcontroller code, upgrading 67

Index

- models and components 62
 - mounting 121
 - ports 63
 - power on 124
 - power outlets 64, 124
 - powering on 124
 - setting up 121
 - shipping box content 119
 - KVM port
 - access, assigning 189, 190
 - alias 184
 - connecting 306
 - connections, sharing 333
 - connections, OSD 324
 - disabling 184
 - enabling 184
 - logins, specifying authentication method 168
 - logins, specifying authentication 168
 - permissions hierarchy 33
 - permissions, understanding 32
 - power management, configuring 175, 182
 - KVM ports 13, 388
 - connect computers to 80
 - connecting computers to 78
 - controlling power while connected to 49
 - enable direct access to 166
 - enabling direct access to 166
 - modifying individual 174, 180
 - syslogging for 218
 - KVM ports screens 388
 - KVM RP
 - beep 422
 - connectors 69
 - powering on 131
 - shipping box contents 129
 - KVM session keyboard shortcuts, to redefine 167
 - KVM terminator usage and types 59
 - KVM terminators 74, 120
 - KVM unit
 - adding cascaded 177
 - configuring cascaded 176
 - connecting cascaded 125
 - deleting cascaded 180
 - editing cascaded 178
 - KVM ports, authentication method 197
 - KVM-connected devices, powering on 124
 - KVM-connected server, controlling power 331
- ## L
- LAN 338
 - LDAP 198
 - Ldap 409
 - LDAP authentication server, to identify an 201
 - LED status 6
 - LEDs 17
 - LEDs on ports 17
 - LEDs on the KVM Expander 64
 - LEDs, front panel activity 19
 - Left / Right 348
 - Level 0 193
 - Level 1 193
 - Level 2 193
 - Load Configuration 417
 - Load from FTP 417
 - Local (“Left”) 244
 - local GMT 258
 - Local ID 370
 - Local IP 370
 - Local IP Address, PPP configuration 255
 - local KVM connection, closing a 332
 - local KVM port connections through the OSD, controlling 324
 - Local NextHop 370

- Local Subnet 370
- local User 1, configure 172
- local User 2, configure 172
- local user and IP users 169
- local work station, to connect the RP to the 131
- local, hot keys for 325
- LOG 226
- Log Level 240
- Log Prefix 240
- log target 230
- logging into
 - console 85
 - OSD 89, 349, 350
 - Web Manager 138
 - Web Manager as a regular user 288
 - Web Manager as admin 138
 - Web Manager, prerequisites for 288
- logging to syslog servers, prerequisites for 55
- logging, configuring 56
- Login Attribute 411
- login screen
 - direct logins enabled
 - IP address and port entered 302
 - IP address entered 302
 - Direct Logins Not Enabled 301
- login screen, to connect to a KVM port through the 306
- login screen, Web Manager 299
- logins through KVM ports, to configure an authentication method for 197
- logins, authentication method 168, 196
- logins, authentication servers 198
- logins, simultaneous 22
- logins, specifying authentication for KVM port 168
- Low BW LAN 338
- Low Color 339
- Low Grey Scale 339

M

- main menu, OSD 350
- managing power, options for 48
- manually, to set the date and time 257
- Mask field 226
- Mean Temp 269
- Memory 418
- menu
 - after connecting to a port, to return to the connection 327
 - Configure, OSD 353
 - Connection 338, 351
 - Network Configuration/ 360
 - options 336
 - OSD main 350
 - Power Management 352
 - System Info 418
 - to connect to servers through the OSD connection 323
- menus and forms in Expert mode, overview of 152
- messages, facility numbers for syslog 55
- Metric 253, 383
- microcode
 - FTP download 279
 - reset 281
 - reset after upgrade 281
 - upgrade 278
 - upgrade, finding pathname for 276
- microcontroller code, upgrading the KVM Expander 67
- mode
 - Expert 151
 - Expert overview 152
 - procedures in Wizard 142
 - steps in Wizard 142
 - Wizard 141
- models and components, KVM Expander 62
- modem
 - connecting an external 114

Index

- connections 342
 - to an AUX port, to connect an external 114
 - to configure the AUX 2 port for use with an external 254
- modem (PCMCIA) card, configuring a 219
- modem card, to configure a 219
- Modem Initialization, PPP configuration 255
- modes, administrative 141
- modify
 - group 188
 - IE security settings 108
 - in-band (RDP) server 209
- modifying individual KVM ports 174, 180
- monitor mode
 - boot alternate image 428
 - boot in u-boot 428
 - boot single user mode 429
 - changing the boot image in u-boot 427
 - replace boot image, network boot 429
- monitor, temperature 8
- monitoring temperature 267
- monitoring temperatures 57
- more information, obtaining 137
- mounting
 - brackets 74, 120
 - KVM Expander, the 121
 - KVM/net 75
- mouse conflicts
 - Windows 2000 / Me 106
 - Windows 95/98/NT 106
 - Windows XP/Windows 2003 105
- mouse conflicts, preventing 105, 106, 107
- mouse, resetting 330
- Mouse/Keyboard 387
- MTU/MRU, PPP configuration 256

N

- Name 380
- navigate
 - conventions for showing how to xxxv
- navigating the OSD 348
- navigation actions, common 349
- navigation keys, basic 348
- Netmask 362, 382
- network 213
- Network bits/sec 336
- network boot in u-boot monitor mode, to replace a boot image from a 429
- network configuration menu options 360
- network configuration screens 361
- network configuration, making a direct connection for 82
- network configuration, performing basic 84
- Network IP 252
- Network Mask 252
- network parameters
 - OSD 92
 - Web Manager 143
 - wiz command 86
- network time protocol 94
- new software version, downloading 425
- next port 314
- NextHop, Local 244
- NextHop, Remote 244
- NIS 198, 414
- NIS authentication server, to configure a 204
- No Encryption 339
- notifications 53
- NTLM 198
- NTP, to set the time and date with 258
- numbers for syslog messages, facility 55
- numbers of cascaded KVM devices, reading the port 306

numbers, example of using facility 55
numeric protocol fields 227

O

OID 247
ordering
 parts 120
ordering options 20
ordering parts 74
organization,
 document xxxii
OSD
 change a password in 90
 configuration screen series,
 understanding 356
 configuring basic networking 88
 configuring networking 92
 connecting to servers through 322, 324
 connection menu, to connect to servers
 through the 323
 conventions for showing how to navigate
 to screens xxxv
 log into 89, 350
 logging in to 349
 main menu 350
 navigating the 348
 RP 421
 through the AlterPath KVM RP,
 controlling the 420
 time and date, setting 95
 to the local computer, to switch the KVM
 RP video display from the 421
OSD Reboot screen 351
Outlets at Device field 183
Outlets Manager 155
outlets, configuring users for managing 158
outlets, KVM Expander 64
Output Interface 230, 378

OUTPUT packet 224
overview, Configure menu, OSD 353
overview, Expert mode 152

P

packet filtering 44
packet filtering rule, to add a 234
Page Up / Page Down 348
panel activity LEDs, front 19
parameters defined using the wiz command,
 to apply and confirm the network 87
parameters using the OSD, to configure
 network 92
Parity, PPP configuration 255
Password 411
password
 changing a 147
 changing a user's 187
 changing admin's default 98
 changing default 98, 99
 changing the root 98
 changing through console 85
 changing through OSD 90
 changing your 291
Password field 186
pathname for firmware upgrades 276
pathname for microcode upgrades 276
PCMCIA card
 ejecting 222
 installing 113
 removing 114
 slots 5
PCMCIA Modem 405, 406
PCMCIA screens 404
performing basic network configuration 84
Permission, SNMP 248
Permissions for username
 403

Index

- permissions hierarchy, KVM port 33
- permissions, port 31
- permissions, understanding KVM port 32
- PM
 - connecting AlterPath 116
 - connecting multiple 117
 - power control of devices 290
 - upgrade 161
- port
 - access 189, 190
 - alias 184
 - AUX 114
 - AUX 1 116
 - AUX 1, configuration 254
 - AUX 2, configuration 254
 - cascaded KVM devices 306
 - connecting to KVM 306
 - connection, quitting 317
 - connections
 - encryption on 194
 - OSD 324
 - sharing KVM 333
 - console 82
 - disabling KVM 184
 - enabling KVM 184
 - information, viewing connected 312, 327
 - logins, authentication method 168
 - permissions 31
 - permissions hierarchy, KVM 33
 - permissions, understanding KVM 32
 - power management, configuration 175, 182
 - resuming connection 317
 - status 264
 - User 1 83
- Port Info 387
- ports
 - access types 40
 - activity LEDs on 17
 - AUX 16, 253
 - connecting computers to the KVM 78
 - controlling power while connected to KVM 49
 - cycle between 313
 - enabling direct access to KVM 166
 - KVM 13
 - modifying individual KVM 174, 180
 - stop cycling between 313
 - TCP 28
 - types of 10
- ports and specify message filtering, to configure syslogging for KVM 218
- ports on cascaded KVM devices, accessing 30
- ports on the KVM Expander 63
- ports screens, AUX 390
- ports screens, KVM 388
- power connector 13
- power control 290
- Power Management 351, 386
- power management 46, 339
 - configuring a KVM port for 175, 182
 - forms 48
 - IPDU 154
 - KVM-connected servers 49, 331
 - menu 352
 - options 48
 - regular users 290
 - setting up and configuring 47
 - Web Manager 48
- Power Outlet 389
- power outlets
 - on the KVM Expander 64
 - to configure users to manage specific 158
- power outlets, configure users to manage 158
- power outlets, KVM Expander 124
- power switch 13
- power, supplying to the KVM RP 131

- powering KVM RP 131
- powering on
 - connected devices 83
 - KVM-connected devices 124
 - the KVM Expander 124
 - the KVM RP 131
 - the KVM/net 83
- PPP 405
- PPP connection from a remote computer, to make a 345
- PPP connection on a remote computer, to configure a 343
- PPP Options, PPP configuration 256
- preconfigured KVM/net, setting up 104
- preconfiguring the KVM/net 103
- prerequisites for
 - accessing in-band servers 298
 - accessing KVM servers 299
 - in-band access 208
 - logging to syslog servers 55
 - using the Web Manager 27
 - Web Manager loggins 288
- Pre-Shared Secret, Local 245
- previous server, switch to 329
- procedures
 - firewall configuration 231
 - in Wizard mode 142
- Profile, PPP configuration 255
- Protocol 369, 376
- protocol 226
- protocol fields
 - ICMP 228
 - numeric 227
 - TCP 227
 - udp 228
- Protocol Number 376
- Protocol pull-down menu 226

- PSH 227
- PSH Flag 377

Q

- Quit 386
- Quit this session 333
- quitting the port connection 317

R

- RADIUS 198
- Radius 412
- Radius authentication server 205
- RC4 193
- RDP servers, prerequisites for access 208
- reboot 284, 419
- reboot, remote location 284
- recommended settings 335
- redefine KVM session keyboard shortcuts, to 167
- redefining hot keys, summary of tasks for 43
- redefining keyboard shortcuts (hot keys) 42
- redefining KVM connection hot keys 42
- redefining KVM connection keyboard shortcuts (hot keys) 166
- redefining sun keyboard equivalent hot keys 42
- refreshing Access window 316
- regular users
 - log into Web Manager as 288
 - power management for 290
 - Web Manager for 286
- REJECT 226
- reject target 231
- remote
 - computer, configure a PPP connection 343

Index

- computer, make a PPP connection 345
- installation 103
- location, to reboot from a 284
- Remote (“Right”) 244
- Remote ID 370
- Remote IP 370
- Remote IP Address, PPP configuration 256
- Remote Nexthop 371
- Remote Subnet 371
- remove a PCMCIA card 114
- replace boot image 429
- resetting
 - IPDU information 157
 - keyboard and mouse 316
 - microcode 281
 - the keyboard and mouse, to 330
 - the microcode after upgrade, to 281
- restore factory default configuration 430
- resume connection after idle timeout 317
- Retries 413
- retrieve configuration data 273
- return to the connection menu after
 - connecting to a port, to 327
- Rivest Cipher four 193
- root password, changing the 98
- Route 252
- routes, static 251, 380
- RP
 - access the KVM/net 420
 - beep 422
 - connecting to KVM/net 130
 - connecting to local work station 131
 - connectors on back 69
 - installing 130
 - powering on 131
 - shipping box contents 129
 - supplying power 131
 - video display, switching 421
- RSA Key, Local 244
- RSA Key, Remote 244

- RST 227
- RST Flag 377
- rule and edit rule options, add 225
- rule for IP filtering, to add a 236
- rule for IP filtering, to edit a 233
- rule options, add rule and edit 225
- rule, to add a packet filtering 234
- rules
 - add 225

S

- Save changes 349
- Save Configuration 416
- save configuration changes, to 140
- Save to FTP 417
- save/load configuration screens 415
- saving changes, logging into the Web Manager and 138
- Scr. saver timeout screen 386
- screen brightness and contrast, adjusting 314
- screen brightness and contrast, to adjust 315, 329
- Screen Save Timeout field 170
- screen series, understanding OSD configuration 356
- screens
 - authentication 407
 - AUX ports 390
 - date/time configuration 383
 - general configuration 357
 - hosts configuration 379
 - IP filtering configuration 372
 - KVM ports 388
 - network configuration 361
 - OSD
 - conventions for showing how to navigate to screens xxxv
 - PCMCIA 404

- save/load configuration 415
- SNMP configuration 364
- static routes configuration 380
- syslog 403
- user station 384
- users and groups 396
- VPN configuration 368
- Secret 412
- Secure (on/off) 411
- security 49, 193
- security settings, IE 108
- sensor, temperature 266
- server
 - add or modify an in-band (RDP) 209
 - connect to 153
 - connect to next 329
 - connect to previous 329
 - controlling power of a KVM-connected 331
 - cycle by 328
 - download microcode from an FTP 279
 - in-band (RDP), delete an 212
 - Kerberos authentication, configuring 199
 - LDAP authentication, configuring 201
 - next 329
 - NIS authentication, configuring 204
 - previous 329
 - Radius authentication, configuring 205
 - RDP, delete an 212
 - SMB(NTLM) authentication, configuring 203
 - syslog, add a 150
 - syslog, delete a 150
 - TACACS+ authentication, configuring 206
- server access, in-band 4
- server connections
 - Access window, managing with 310
 - AlterPath Viewer options 337
 - in-band and out of band 36
 - sharing 317, 319
 - simultaneous 23
 - what you see 295
- server drop-down list 305
- Server IP 410, 414
- Server name 389
- servers
 - administering users of connected 40
 - configuring in-band (RDP) 207
 - connecting, OSD 322
 - connecting, Web Manager 304
 - cycling between 328
 - identifying in list 305
 - prerequisites for in-band access to RDP 208
 - prerequisites for logging to syslog 55
 - syslog 55
 - servers with in-band connections, prerequisites for accessing 298
 - servers with KVM connections, prerequisites for accessing 299
 - servers, authentication 198
 - services 223
 - session keyboard shortcuts, to redefine KVM 167
 - session, to kill an active 283
 - sessions information, to view active 282
 - sessions, active 282
 - Set 227
 - set the time and date with NTP 258
 - Set, TCP flag 227
 - setting AlterPath Viewer options 337
 - setting date and time manually 257
 - setting time and date, OSD 95
 - setting up
 - KVM Expander 121
 - KVM/net 75
 - power management 47
 - preconfigured KVM/net 104

Index

- terminal emulator dial up connection 345
- settings
 - AlterPath Viewer 335
 - avoiding conflicting mouse 105
 - change network, to 143
 - configure host, to 215
 - host 214
 - modify IE security, to 108
 - recommended Alter Path Viewer 335
- share a server connection, to 319
- sharing a server connection 317
- sharing KVM port connections 333
- Shell field 187
- shipping box contents
 - AlterPath KVM/net 73
 - KVM Expander 119
 - KVM RP 129
- shortcuts
 - redefine KVM session keyboard, to 167
 - redefining keyboard 42
 - redefining KVM connection keyboard 166
- Show Frames/sec 336
- Show Startup Dialog 336
- Smb(NTLM) 413
- SMB(NTLM) authentication server, to configure an 203
- SNMP 245
- SNMP Configuration 366
- SNMP configuration screens 364
- SNMP, to configure 245
- SNMPv1/v2 Community 366
- SNMPv1/v2 or v3 OID 367
- SNMPv1/v2 or v3 Permission 367
- SNMPv1/v2 Source 367
- SNMPv3 Password 367
- SNMPv3 Username 367
- software upgrade 160
- software version, downloading a new 425
- Source IP 375
- Source IP field 226
- Source Mask 375
- Source Port 227, 376
- Source, SNMP 247
- static routes 251
- static routes configuration screens 380
- status, LED 6
- status, port 264
- status, viewing port 264
- Step 1 Network Settings 142
- Step 2 Access 144
- Step 3 System Log 149
- steps in Wizard mode 142
- Stop Bits, PPP configuration 255
- stop cycling 313
- Subnet Mask, Local 244
- Subnet Mask, Remote 244
- Sun Keyboard 358
- sun keyboard equivalent hot keys 42
- sun keyboard keys 326
- Switch Next 387
- Switch Previous 387
- switch, power 13
- SYN 227
- SYN Flag 376
- SysContact 246, 366
- SysLocation 246, 366
- syslog 217
- Syslog Facility 357
- syslog files for IPDUs, to configure creation of alarms and 160
- syslog messages, facility numbers for 55
- syslog screens 403
- syslog server, to add a 150
- syslog server, to delete a 150
- syslog servers 55
- syslog servers, prerequisites for logging to 55

- syslogging for KVM ports and
 - specify message filtering, configure 218
- syslogging, enhanced 9
- system 256
- System Info 351
- system info menu 418
- system information, to access 419
- system information, viewing 263

T

- T1 338
- Tab 348
- tab, to connect to another port using the
 - current AlterPath Viewer and Access window 312
- tables, host 249
- TACACS+ 198
- TACACS+ authentication server, to identify
 - a 206
- TacacsPlus 412
- Target 375, 382
- target pull-down menu options 225
- target, log 230
- target, reject 231
- tasks for redefining hot keys, summary of 43
- tasks related to access to connected devices
 - 40
- tasks, additional configuration 104
- tasks, common 134
- TCP Flags 227
- TCP flags
 - ACK 227
 - Any 227
 - FIN 227
 - PSH 227
 - RST 227
 - Set 227
 - SYN 227
 - Unset 227
 - URG 227
- TCP Options 240
- TCP Port Viewer 359
- TCP ports 28
- TCP protocol fields 227
- TCP RDP Ports 359
- TCP Sequence 240
- TCP Viewer Ports 171
- tcp-reset 241
- temperature monitor 8, 267
- temperature sensor 266
- temperatures, monitoring 57
- ten concurrent users, support for up to 4
- terminal emulator, dialing in 346
- terminal emulator, setting up 345
- terminators, KVM 59
- time and date using the OSD, to set the 95
- time and date with NTP, to set the 258
- Time screen 418
- time, GMT 258
- time, setting manually 257
- time/date 257
- Timeout 412
- timeout, to resume your port connection after
 - an idle 317
- Toggle Full Screen 336
- tools for specifying authentication methods
 - 52
- Triple Data Encryption Standard 193
- turn the beeper on or off when switching
 - between the local and the remote work stations, to 422
- type and its supported functionality,
 - determining the connection 38
- type in the connect to server drop-down list,
 - identifying servers and their connection 305
- Type of user 398
- types of access to ports 40

Index

types of KVM terminators 59
types of ports 10
types of users 21
typographical conventions xxxiv

U

u-boot monitor mode 428, 429
u-boot monitor mode, changing the boot image in 427
udp protocol fields 228
understanding KVM port permissions 32
understanding OSD configuration screen series 356
Unit boot from 261
Unset 227
Up / Down 348
up a terminal emulator dial up connection, .to set 345
up and configuring power management, setting 47
up connection, .to set up a terminal emulator dial 345
up the KVM Expander, setting 121
upgrading
 Cyclades pathname 276
 firmware 274, 277
 firmware AlterPath PM 161
 KVM Expander microcontroller code 67
 microcode 278
 resetting microcode after 281
 software 160
URG 227
URG Flag 377
User 411
user
 add 145, 186
 delete 147
 log in as regular 288

user (KVM over IP) sessions, to configure IP 173
User 1 and User 2 sessions, to configure local 172
User 1 management port, to connect to the 83
User 2 sessions, to configure local User 1 and 172
user access 68
user and IP users, local 169
User Database Enter the username 398
user mode from u-boot monitor mode, to boot in single 429
User Name field 186
user or group, to assign KVM port access to a 190
user or group, to delete a 187
user station screens 384
user's password, to change a 187
User1 connection 418
User2 connection 418
users
 local user and IP 169
 managing power outlets 158
 of connected servers 40
 power management for regular 290
 simultaneous 4
 types of 21
 Web Manager for regular 286
users & groups 185
users and groups for assigning KVM port access, to select 189
users and groups screens 396
Users Manager form 158

V

Version 418
version, downloading a new software 425
Video 387

- view
 - active sessions information, to 282
 - and reset IPDU information, to 157
 - connected port information, to 312, 327
 - general information 263
 - IPDUs info 157
 - port status, to 264
 - Viewer and Access window tab, to connect to another port using the current AlterPath 312
 - Viewer Options 336
 - Viewer options, setting AlterPath 337
 - Viewer settings, AlterPath 335
 - Viewer, to connect to the previous or next authorized port without opening a new AlterPath 314
 - viewing in-band connections 298
 - viewing KVM connections 296
 - viewing system information 263
 - VPN 241
 - VPN configuration screens 368
 - VPN, to configure 242
- W**
- Watchdog Timer 261
 - changing admin's default password 98
 - Web Manager 26
 - access without direct connection 100
 - completing configuration using the 97
 - Connect to Server form 308
 - connecting to servers through the 304
 - conventions for showing how to navigate to forms xxxv
 - for regular users 286
 - IPDU Power Management forms 48
 - logging as as a regular user 288
 - logging as as admin 138
 - login screen 299
 - prerequisites for logging into 288
 - prerequisites for using 27
 - to use a dynamic IP address to access the 101
 - to use the default IP address to access the 100
 - Web Manager, logging into the 138
 - what's new in KVM/net 4
 - wiz command
 - apply network parameters 87
 - configure network parameters 85, 86
 - wiz command, configuring basic networking 85
 - Wizard mode 141
 - Access (Step 1) 144
 - Network Settings(Step 2) 142
 - procedures in 142
 - steps in 142
 - System Log (Step 3) 149
- Y**
- yMax Value 269
 - yMin Value 269