

AlterPath™

Advanced Console Server

User Manual



cyclades

Cyclades Corporation

3541 Gateway Boulevard

Fremont, CA 94538 USA

1.888.CYCLADES (292.5233)

1.510.771.6100

1.510.771.6200 (fax)

<http://www.cyclades.com>

Release Date: July 2005

Part Number: PAC0379

© 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

Before You Begin v

Audience	vi
Document Organization	vi
Related Documents	vii
Typographical Conventions	vii
Naming Conventions	viii
Cross References	ix
Additional Resources	ix
Cyclades Technical Training	ix
Cyclades Firmware Upgrades	ix

Chapter 1: Introduction..... 1

ACS Access and Configuration	2
Product Models and Components	2
ACS Setup Diagram	4

Chapter 2: Installing the ACS..... 5

Package Contents.....	6
Rack Mounting the ACS	10
System Requirements	11
Default Configuration Parameters	12
Pre-Install Checklist	12
Installation and Configuration Process	13
Installation	13
Network Parameters	14
Configure the ACS in Wizard Mode	19
Test the Configuration	19
Configure the ACS in Expert Mode	19

Save the Changes	19
Chapter 3: ACS for Regular Users	21
Using the Web Manager	22
Using the Command Line Interface (CLI)	24
Logging into the Terminal	25
Telnet Access	25
SSH Access	25
ts_menu Access	26
Power Management	27
Security	28
Chapter 4: Web Manager for Administrators	31
Overview	32
Logging In	32
ACS Web Manager: Elements	34
Wizard Mode	34
Expert Mode	35
Button Functions	36
Saving Your Configuration	37
Configuring the ACS in Wizard Mode	38
Security Profile	38
Network Settings	41
Port Profile	43
Access	45
Data Buffering	49
System Log	52
Configuring the ACS in Expert Mode	53
Expert Mode Menu	53
Applications	56
Connect	56
Power Management	57
Terminal Profile Menu	65
Network	67
Host Settings	68

Syslog	71
PCMCIA Management	72
What is VPN	78
VPN Connections	80
SNMP Daemon Settings	82
Firewall Configuration	86
Host Table	95
Static Routes	97
Security	99
Users and Groups	99
Active Ports Sessions	102
Security Profile	103
Ports	106
Physical Ports	106
General Port Configuration	108
Access - Power Management	110
Access - User and Group Setup	111
Data Buffering	115
Multi-User	116
Power Management	118
Other Setting	120
Virtual Ports	121
Ports Status	124
Administration	125
System Information	125
Notifications	126
Time / Date	132
Manual Setting	132
Setting Network Time Protocol (NTP)	132
Boot Configuration	133
Backup Configuration	135
Upgrade Firmware	138
Reboot	140

Appendix A: Hardware Specifications	141
Appendix B: Safety Guidelines	143
Safety Guidelines for Rack-Mounting the ACS	144
Safety Precautions for Operating the ACS	145
Working inside the AlterPath Console Port Server	146
Replacing the Battery	146
FCC Warning Statement	147
Notice About FCC Compliance for all Alterpath ACS Models	147
Canadian DOC Notice	147
Aviso de Precaución S-Mark Argentina	148
Trabajar dentro del AlterPath Advanced Console Server	149
Batería	149
Appendix C: Supported Browsers and JRE	151
Supported Web Browsers	152
Installing JRE	152
Tested Environments	152
Installation Requirements	152
Installing From Windows Internet Explorer	152
Installing From Windows Netscape or Mozilla	153
Glossary	155
Index	171

Before You Begin

This manual is designed to guide you in installing and configuring the AlterPath Advanced Console Server through the ACS Web Manager. It also provides other necessary information to guide you in your day-to-day operations of the ACS.

Audience

This manual is intended for System administrators and regular users who are responsible for the daily administration and operation of the AlterPath Advanced Console Server using the Web Manager interface.

While users may use any available method to configure the ACS, the ACS Web Manager is primarily designed for users who are new to Linux or UNIX with a primarily PC/Microsoft background.

The user is expected to have a basic knowledge of networking and using a graphical user interface.

For users who wish to configure ACS using vi, or Command Line Interface (CLI), or read about other advanced features of the ACS, please refer to the *ACS Advanced Administration Guide*.

Document Organization

This manual is organized as follows:

- | | |
|-----------------------------------|---|
| 1: Introduction | Defines and explains the overall product features and uses of ACS. |
| 2: Installing the ACS | Explains the procedure for installing and setting up ACS. |
| 3: ACS for Regular Users | Explains how to access devices and operate the web interface. This chapter is designed for the ACS regular user. |
| 4: Web Manager for Administrators | Presents the procedures for configuring the ACS, using the web interface. All the procedures follows the menu structure of the entire web interface in Wizard Mode and Expert Mode. |
| Appendix A | Summarizes the Hardware Specifications of the AlterPath Advanced Console Server. |
| Appendix B | Outlines the Safety Considerations for installing and handling the ACS. |
| Appendix C | Lists the latest Web Browsers that ACS supports, and explains the procedure for installing JRE on your PC. |

Glossary	Contains a glossary of terms and acronyms used in the manual.
Index	Index of keywords or subjects.

Related Documents

The following documents for the Cyclades AlterPath ACS is shipped with the product.

- AlterPath ACS Quick Start Guide (hard-copy)
- AlterPath ACS Advanced Administration Guide

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

A hard-copy version of this document can be ordered under part number PAC0379 through your Cyclades sales representative.

Typographical Conventions

Form/Window labels	Words that appear on forms, windows, or any part of the user interface are typed in boldface . <i>Examples:</i> The Add User dialog box; the Password field.
Hypertext links	With the exception of headings and the Table of Contents (which are already linked), all <u>underlined</u> words are hypertext links.
Important words	For emphasis, important words are <i>italicized</i> .
Menu selections	The order in which you select a menu is indicated by the “greater than” symbol (>). <i>Example:</i> Network > Access Method .
Screen words	Words that appear as part of the graphical user interface are typed in boldface . <i>Examples:</i> The Configuration window; the Password field.

Untitled Data Fields	Some data entry fields of the GUI windows or forms do not have titles. When this field is described in any field definition section of the manual, the field is indicated as untitled, enclosed in angled brackets. <i>Example:</i> [untitled] Type in the port number in this field.
Untitled forms	While most forms are identified by it's menu selection, some forms do not bear the title. The manual uses initial capitals to refer to their names or titles. <i>Examples:</i> The Data Buffering form; the VPN Connections form; the Active Ports Session form.
User entry words	Words or characters that you would type in are shown in <i>courier</i> . <i>Example:</i> myPas8word
Window levels	Screen levels are also indicated by the “greater than” symbol (>), starting from parent to child to grandchild and so forth. In ACS, the navigable window types are the forms and the dialog boxes. <i>Example:</i> Security > Users and Groups > Add

Naming Conventions

ACS	Short name for the Cyclades AlterPath Advanced Console Server.
Dialog box	The dialog box is a pop up window that appears and prompts for user input as part of the process for completing a form in order to configure the ACS.
Form	The form is the largest part of the user interface; it contains the user selection or input fields for each selected item in the menu.

Form names	The name or title of a form may not necessarily appear on the actual form. When this is the case, the form is named after its menu selection or form function.
Select	To <i>select</i> is the same as to <i>click your mouse</i> .

Cross References

The ACS User Manual cross-references the following Cyclades documents:

- ACS Advanced Administrator Guide
- AlterPath Manager Manual
- Cyclades Power Management Manual

To access Cyclades product documentation, including release notes and updates, please visit the Cyclades web site at:

www.cyclades.com/support/downloads.php

Additional Resources

The following sections describe Cyclades offerings, including technical training and firmware upgrades.

Cyclades Technical Training

Cyclades offers a suite of technical courses to increase your knowledge of the AlterPath ACS.

To learn more about Cyclades Technical Training Center and offerings, please visit our website at www.cyclades.com/training, call us at 1-888-292-5233, or send an email to training@cyclades.com.

Cyclades Firmware Upgrades

Cyclades offers periodic firmware upgrades for the AlterPath ACS. These upgrades are available free of charge to current Cyclades customers. Visit <http://www.cyclades.com/support/downloads.php#acs> to download the latest firmware.

Chapter 1

Introduction

The AlterPath Console Server (ACS) comes from Cyclades' line of Console Access and Terminal Servers designed to allow local and dial-in access for in-band and out-of-band network management.

Modeled after the Cyclades-TS line of console server, the ACS adds the following advanced features:

- PCMCIA slots that support standard interface cards (Ethernet, Modem, and wireless LAN).
- Optional dual entry redundant power supply (AC/DC) for extra reliability.
- Secure clustering for up to 1024 devices, SSH v2, RADIUS authentication, IPSec, IP filtering, and user access lists per port.
- Console management supports Windows Server 2003 EMS protocols.
- Data buffering, Event notification, and a selection of direct access methods to serial ports.

The Alterpath ACS is available in 1, 4, 8, 16, 32 and 48-port models that fit in 1U of rack space. As with most Cyclades products, the ACS runs an embedded version of the Linux operating system.

ACS Access and Configuration

You can access the ACS using any of the following three methods:

- Web Browser
- Console directly connected to the ACS
- Telnet/SSH over a network

You can configure ACS by using any of the following user interfaces:

- Web Browser
- VI Editor
- Wizard
- Command Line Interface (CLI)

With the ACS set up as a Console Access Server, you can access a server connected to the ACS through the server's serial console port from a workstation on the LAN or WAN.

There is no authentication by default; you can configure the system for authentication to be performed by a Radius server, a TacacsPlus server, or even by a local database. You can use either Telnet or ssh (a secure shell session).

Product Models and Components

There are two models of the ACS based on the type of power supply:

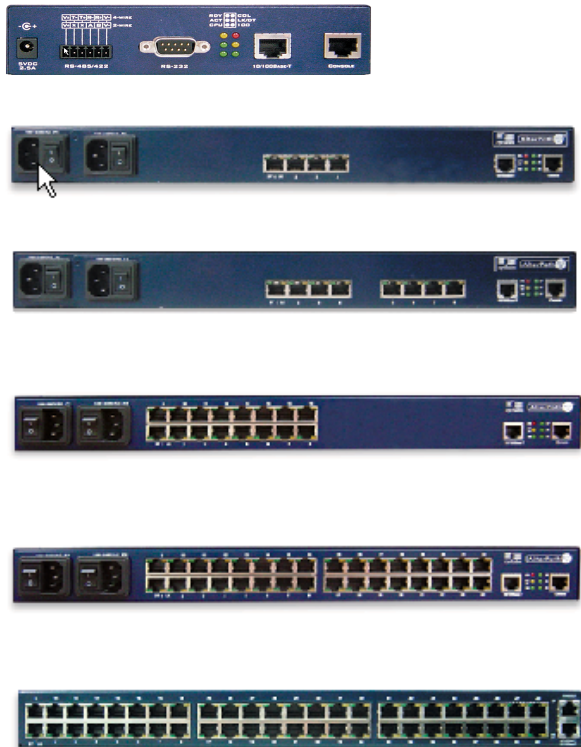
- ACS with a dual power supply and two PCMCIA slots
- ACS with a single power supply and two PCMCIA slots.

Product Models and Components

There are six models of the ACS based on the number of serial ports:

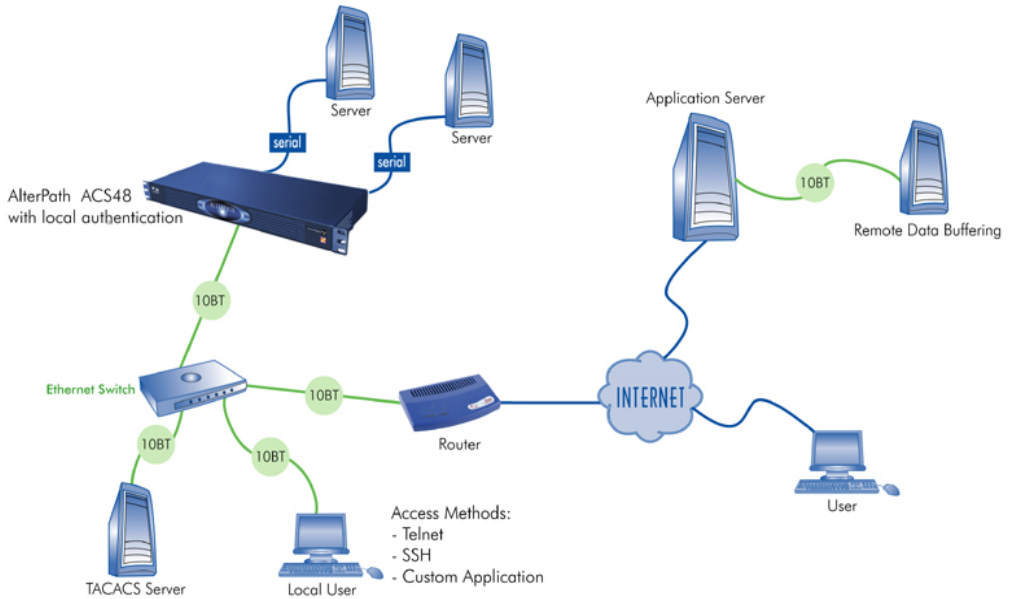
- ACS48
- ACS32
- ACS16
- ACS8
- ACS4
- ACS1

The figure below shows AlterPath ACS1 through ACS48.



ACS Setup Diagram

The diagram below shows a typical setup of the AlterPath Console Server.



Chapter 2

Installing the ACS

This chapter presents the procedures for installing and setting up the ACS and is organized as follows:

- Package Contents
- Rack Mounting
- Installation and Configuration Process

Note: For configuration procedures using vi or CLI, refer to the *AlterPath ACS Advanced Administration Guide*.

Package Contents

There are six models of the AlterPath Advanced Console Server based on the number of serial ports:


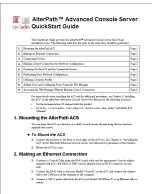
- ACS48
- ACS32
- ACS16
- ACS8
- ACS4
- ACS1






All models are available with either a single (A/C or VDC) or double (A/C or -48 VDC) power supply.







The shipping box contains the AlterPath Advanced Console Server 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 checkboxes to check off each item, and you can use the part numbers from this table to reorder any of the parts.







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


Table 2-1: Shipping Box Contents, Part Numbers, and Description

R	Item	P/N	Description	Purpose
1. <input type="checkbox"/>		PAC0266	Documentation CD	PDF copies of this guide and all other Cyclades product documents.
2. <input type="checkbox"/>		PAC0199	<i>AlterPath ACS QuickStart Guide</i>	Basic installation guide in printed format. Written for users experienced in installing Cyclades products.

R	Item	P/N	Description	Purpose
3.			Power cable. Two cables are included for the dual power supply units.	To connect the ACS to a power source. The destination country is used to determine which type of cord is shipped based on the country's standard power outlet. The prongs of available cords are shown in the following rows. Talk with a Cyclades sales representative if the power cable you need is not listed in this table or if you have special requirements.
		CAB0010	NEMA5--15P. Flat blades with round grounding pin.	United States and other countries.
		CAB0037	Schuko. Round pin attachment plug.	European and other countries.
		CAB0055	Oblique flat blades with ground.	Australia, New Zealand, and other countries.
		CAB0056/ CAB0104	Rectangular blade plug.	UK, Ireland, and other countries.

R	Item	P/N	Description	Purpose
		CAB0278	Flat blades with round grounding pin.	Japan.
4. <input type="checkbox"/>		ADB0017	RJ45 to DB25F crossover adapter	To connect the console port to a computer that has a DB-25 male connector.
5. <input type="checkbox"/>		ADB0025	RJ45 to DB25M crossover adapter	To connect the console port to a computer that has a DB-25 female connector.
6. <input type="checkbox"/>		ADB0036	RJ45 to DB9F crossover adapter	To connect the console port to a computer that has a DB-9 connector.
7. <input type="checkbox"/>		ADB0039	Sun/Netra crossover adapter	To connect the console port to a Sun Netra server, or other devices with the same pinout configuration.
8. <input type="checkbox"/>		CAB0018	RJ45 to RJ45 7ft. CAT5 cable	Use for the following: <ul style="list-style-type: none"> • To connect a device or an IPDU to a serial port. • To connect an Ethernet port to the LAN. • To connect a terminal to a console port.

R	Item	P/N	Description	Purpose
9. <input type="checkbox"/>		CAB0025	RJ45 to DB25M straight-thru cable	Use for modems and other DCE devices.
10. <input type="checkbox"/>		CAB0042	DB9F to DB25F crossover cable <i>ASCII Only</i>	To connect the RS-232 serial port to a computer that has a DB-25 male connector.
11. <input type="checkbox"/>		CON0071	DB25F Loopback	Use to test and diagnose serial ports.
12. <input type="checkbox"/>		CON0093	DB9F to DB25M adapter <i>ASCII Only</i>	Use to convert serial port connectors.
13. <input type="checkbox"/>		CON0095	3.5mm Block Plug <i>ASCII Only</i>	Use to establish RS-485 connection.
14. <input type="checkbox"/>		HAR0370	2 - Mounting brackets with 8 - screws (2 spares)	Use to mount the ACS to a rack or cabinet. To mount on a wall, order the brackets under part number: HAR0220.

R	Item	P/N	Description	Purpose
15. <input type="checkbox"/>		POW0021	Power Supply +5V/2.5A <i>ACSI Only</i>	Power supply for ACS1.

Rack Mounting the ACS

To rack-mount and connect the ACS to your network, perform the following steps:

1. Install the brackets onto the front or back edges of the box using a screw driver and the screws provided with the mounting kit.



2. Mount the ACS box in a secure position.

Note: Refer to Appendix B: Safety Guidelines section of this manual to ensure safety.

Caution: Install your AlterPath Advanced Console Server near the power managed equipment and where there is an adjacent and accessible wall socket outlet.

3. Proceed to the **Installation and Configuration** section of this chapter.

System Requirements

To configure the ACS, Cyclades recommends any of the following hardware specifications:

- Workstation with a console serial port or,
- Workstation with Ethernet and TCP/IP topology or,
- Cyclades AlterPath Manager.

The following table lists the hardware connectivity required for each configuration method:

Hardware Connectivity	Configuration Method
Workstation, Hub, Ethernet Cables.	Web browser, vi, Wizard, or CLI
Console, Console Cable (constructed from RJ45 straight-through cable + adapter. Workstation, Hub Ethernet Cables.	vi, Wizard, or CLI.

Note: This manual is designed primarily for Web Manager users. If you use vi, the wizard (CLI version), or CLI, refer to the *ACS Advanced Administration Guide*.

Note: To install ACS with AlterPath Manager, refer to the *AlterPath Manager Manual* and configure the device using the AlterPath Manager.

Default Configuration Parameters

- DHCP enabled (if there is no DHCP Server, IP for Ethernet is 192.168.160.10 with a Netmask of 255.255.255.0)
- CAS configuration
- Socket_server in all ports (access method is telnet)
- 9600 bps, 8N1
- No Authentication

Pre-Install Checklist

Before you install and configure the ACS, ensure that you have the following:

Root Access	You will need Root Access on your local UNIX machine in order to use the serial port.
HyperTerminal, Kermit, or Minicom	If you are using a PC, ensure that HyperTerminal is set up on your Windows operating system. If you have a UNIX operating system, you will be using Kermit or Minicom.
IP Address of the PC or terminal, AlterPath ACS, NameServer, and Gateway	You will need to locate the IP address of your PC or workstation, the ACS, and the machine that resolves names on your network. Your Network Administrator can supply you with these. If there is outside access to the LAN that the ACS will be connected with, you will need the gateway IP address.
Network Access	You must have a NIC card installed in your PC to provide an Ethernet port, and have network access.
Java 2 JRE	You must have Java 2 Runtime Environment (JRE) version 1.4.2 (which can be found at http://java.sun.com/) installed on your PC with your browser acknowledged to use it.

Ensure that the browser you are using acknowledges the Java version by following the procedures given in *Appendix C: Supported Browsers and JRE*.

Installation and Configuration Process

The installation and configuration process is divided into six distinct tasks:

- Install ACS and connect to the network.
- Configure the network parameters (using the console port).
- Configure ACS using the Web Manager in Wizard Mode.
- Test Configuration.
- Customize configuration using the Web Manager in Expert Mode.
- Save Changes.

Note: You can configure ACS using the command line interface alone. See the **ACS Advanced Administration Guide** to configure ACS using CLI.

Installation

The following procedure describes the necessary physical connection in order to connect the ACS to the network.

▼ **To Install ACS and Connect to the Network**

1. Plug the power cable into the ACS.
2. Insert the female end of the black power cable into the power socket on the ACS and the 3-prong end into a wall outlet.

Caution: To help prevent electric shock, plug the ACS into a properly grounded power source. The cable is equipped with a 3-prong plug to help ensure proper grounding. Do not use adapter plugs or remove the grounding prong from the cable. If you use an extension cable, use a 3-wire cable with properly grounded plugs.

Caution: The AlterPath Advanced Console Server must be plugged into a receptacle protected by an appropriate, listed circuit breaker.

3. Connect the console cable.

Construct a Console Cable out of the RJ-45 straight-through cable and the appropriate adapter provided in the product box. (All adapters have an RJ-45 connector on one end, and either a DB25 or DB9 connector on the other end, male or female). Connect this cable to the port labeled “Console” on the ACS with the RJ-45 connector end, and connect the adapter end to your PC’s available COM port.

Note: The modem cable is not necessary for a standard installation and configuration. Use it when the configuration is complete and you want to access the box remotely through a serial port.

4. Connect to the Network.

Connect the ACS network port to the Ethernet hub or switch.

Network Parameters

This step is necessary to make ACS visible on the network. The configuration can be done using the console port of the Cyclades ACS or through the network using the default network settings.

▼ *To Configure the Network Parameters Using the Console Port*

- 1.** Install and launch your serial communication software (*e.g.*, HyperTerminal, Kermit or Minicom).

You can obtain the latest update to HyperTerminal from:

<http://www.hilgraeve.com/hpte/download.html>.

If you are using a PC, use HyperTerminal to perform the initial configuration of the ACS directly through your PC’s COM port connected with the ACS. HyperTerminal, which comes with Windows 95, 98, Me, NT, 2K, and XP is often located under **Start > Program > Accessories**. HyperTerminal emulates a dumb terminal when your PC connects to the serial port (console port) of the ACS.

2. Select available COM port.

In HyperTerminal (**Start > Program > Accessories**), select **File > Properties**, and click the **Connect To** tab. Select the available COM port number from the Connection dropdown list box.

3. Configure COM port using the following parameters:

- Serial Speed: 9600 bps
- Data length: 8 bits
- Parity: None
- Stop bit: 1
- Flow control: None

4. Power on the ACS.

After the initial startup scripts, the login prompt appears.

Note: If your ACS model is equipped with dual power supplies, make sure you turn both power switches on. After system initialization, a beep sound may warn if one of the power supplies is off.

5. Connect the COM Port to the ACS Console.

Login as **root**, and enter the default password, **tslinux**.

Caution: Changing the default password closes a security hole that could be easily exploited. It is strongly recommended to change the **root** password before setting up the ACS for secure access to the ACS equipment

6. To Change the root password: Enter the **passwd** command, and enter a new password when prompted.

7. The following Security Advisory appears the first time ACS is accessed.

IMPORTANT - Security Advisory!

Console Management provides critical access to management features of attached equipment. Please take the required precautions to understand the potential impacts this device may have to your SECURITY policies.

From factory, this device is configured as follows:

- Single password for ROOT;
- All serial ports DISABLED,
- DHCP, Telnet, SSHv1 & SSHv2, and HTTP & HTTPS enabled.

Cyclades strongly recommends:

1. To change the “root” password before setting up the box for secure access to the ACS equipment. See Chapter 2, “To Install ACS and Connect to the Network
 2. To select a Security Profile to complete the INITIAL SETUP. Security is dependent on Policy and is Configurable to fit in environments with varying levels of Security. Cyclades provides three pre-set Security Levels: SECURED, MODERATE and OPEN, and in addition, the ability to set a CUSTOM Security Profile. For details on selecting and configuring a Security Profile see Chapter 4, “Configuring the ACS in Wizard Mode. For configuring using CLI, see ACS Advanced Administration Guide.
 3. Do not leave the equipment idle WITHOUT selecting a Security Profile.
 4. To enable Serial Ports and configure them using the Web Manager, see Chapter 4, “Port Profile”. For configuring using CLI, see ACS Advanced Administration Guide.
- 8.** Launch the Configuration Wizard by entering the `wiz` command.
- As shown in the sample screen below, the system brings up the configuration wizard banner and begins running the wizard.

Installation and Configuration Process

```
*****  
***** CONFIGURATION WIZARD *****  
*****
```

Current configuration:

```
Hostname : CAS  
DHCP : disabled  
System IP : 192.168.48.11  
Domain name : cyclades.com  
Primary DNS Server : 192.168.44.21  
Gateway IP : 192.168.48.1  
Network Mask : 255.255.252.0
```

Set to defaults? (y/n) [n] : _

- a. At the prompt, enter **n** to change the defaults.

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

- b. Press Enter to accept the default hostname, otherwise enter your own hostname.

```
Hostname[CAS] :
```

- c. Press Enter to keep DHCP enabled or enter a static IP address.

By default, ACS uses the IP address provided by the DHCP server. If your network does not use DHCP, then ACS will default to 192.168.160.10.

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

- d. Enter the domain name

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

- e. Enter the IP address for the Primary DNS (domain name) server

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

- f. Enter the IP address for the gateway.

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

- g.** Enter the netmask for the subnetwork

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

The network configuration parameters appear.

```
Current configuration:
```

```
Hostname : CAS
```

```
DHCP : disabled
```

```
System IP : 192.168.51.143
```

```
Domain name : cyclades.com
```

```
Primary DNS Server : 129.168.44.21
```

```
Gateway IP : 192.168.48.1
```

```
Network Mask : 255.255.252.0
```

- h.** Enter **y** to the prompts shown in the following screen example.

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

- i.** To confirm the configuration, enter the `ifconfig` command.

Note: For the procedure on how to configure the ACS from **wiz** to support Kerberos tickets, refer to the *ACS Advanced Administration Guide*.

- 9.** After the initial configuration, you can configure the network further by using any of the following methods:

- Web Manager
- Command Line Interface (CLI) via SSH
- AlterPath Manager, if installed on your network.

Note: To use the ACS Web Manager, ask your system administrator for the IP address. By default, ACS uses the IP address provided by the DHCP server. If your network does not use DHCP, then ACS defaults to 192.168.160.10. Configure your ACS to connect to this address and run the Web Manager.

Configure the ACS in Wizard Mode

- Proceed to **Chapter 4: “Web Manager for Administrators”**, and complete the procedure for configuring ACS in Wizard Mode.

Test the Configuration

- Log in as a regular user and connect to a port. Check the other features (for example Data Buffering, Power Management, and so on) as discussed in Chapter 3: “**ACS for regular users**”.

Note: To create new users, see Wizard Mode **Step 3: Access** (page 4-10) of **Chapter 4: “Web Manager for Administrators”**.

Configure the ACS in Expert Mode

Proceed to Chapter 4: **Web Manager for Administrators**, and continue with configuration using the Expert Mode.

Save the Changes

Click on the **apply changes** button located on the bottom of the ACS Web Manager Configuration screen to save your configuration to Flash.

Chapter 3

ACS for Regular Users

This chapter presents the methods for accessing serial ports and the basic operations for using ACS. Addressed to the ACS end user, the chapter is divided into the following topics:

- Using the Web Manager
- Using the Command Line Interface (CLI)
- Using Telnet
- Using the TS Menu
- Power Management

Using the Web Manager

Note: Refer to **Appendix C** for a description of the web requirements for connecting to a serial port.

To use the Web Manager to connect to a serial port, follow the following procedure:

1. Connect your web browser to the ACS by typing in the Console Access Server's IP address (*e.g.*, `https://10.10.10.10`) provided to you by your system administrator in the address field of your internet browser.
2. Press **Enter**.

The system brings up the ACS Web Manager Login Window:

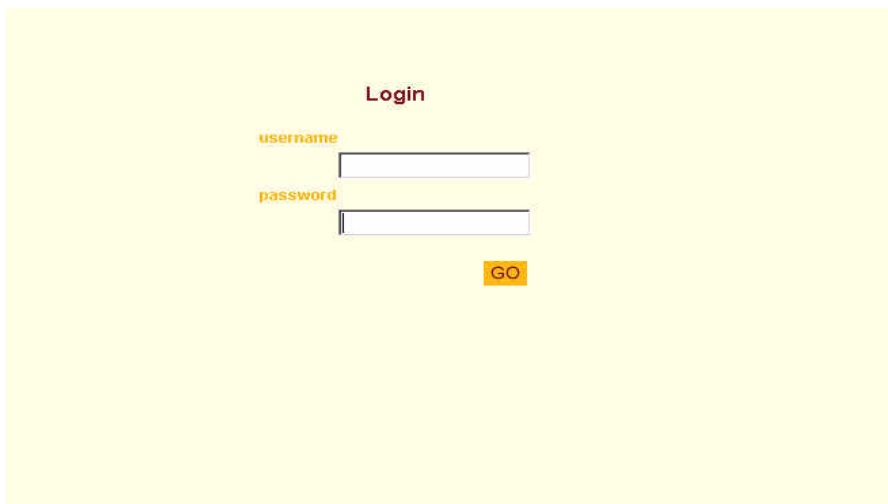


Figure 3-1: Web Manager Login Window

3. To log in, type in your username and password as provided to you by your system administrator. The system brings up the Port Selection form:

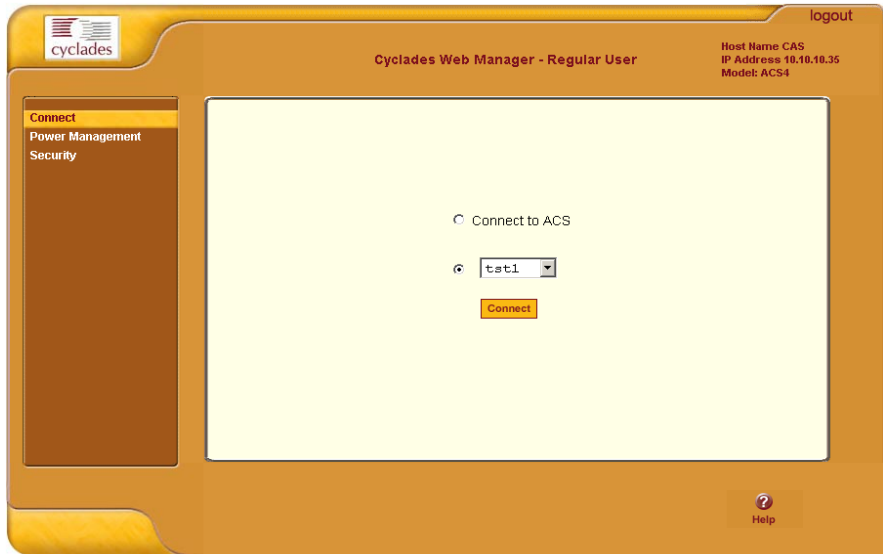


Figure 3-2: Port Selection Window

4. To connect to a port (by default, the radio button is already selected for connecting to Port 1). From the drop down menu select the port to which you wish to connect, and then click on **Connect**.

- OR -

To connect to the ACS box, select the radio button “**Connect to ACS**”, and then click on **Connect**.

Depending on your selection, the system either opens a Java connection to the port selected, or launches an SSHv2 connection to the ACS box.

In the sample screen below, the system displays a Java window after connecting to the selected server.

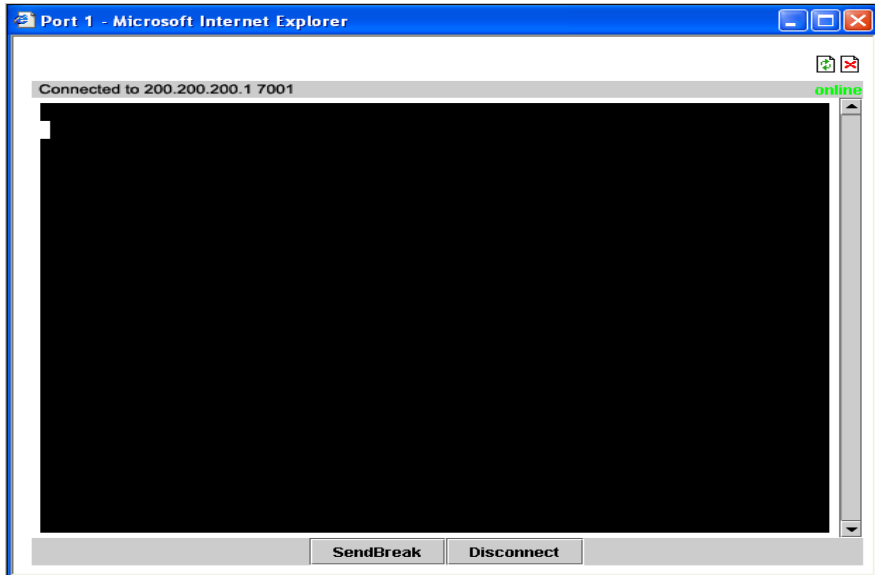


Figure 3-3: SSHv2 or Java Connection

Using the Command Line Interface (CLI)

Operating the terminal varies according to whether the selected port is configured for Telnet access or for SSH access.

To log in, see the log in instructions for Telnet or SSH in the next section of this chapter.

Click in the terminal window and start entering commands.

To send a break to the terminal, click on the **SendBreak** button.

The upper right hand corner of the browser (Java window) shows two icons: **Reconnect & Close**.



Select the left icon to reconnect to the server; select the right icon to end the session or disconnect from the Java window.

Logging into the Terminal

Telnet Access

To open a telnet session to a serial port, enter the following command:

```
telnet <hostname or IP address> <TCP port number>
```

Press ENTER

Where: <hostname> is the hostname configured in the workstation where the telnet client will run (through /etc/hosts or DNS table). Or it can just be the IP address of the ACS (Ethernet's interface) as configured by the administrator or as learned from DHCP.

<TCP port number> is the number associated to the serial port. The factory default values, 7001 corresponds to serial port 1, 7002 to serial port 2 and so forth, and 3000 is a pool with all serial ports.

To close the telnet session, just press the telnet hot key configured in the telnet client application (usually it is "**Ctrl-J**").

SSH Access

Secure Shell (SSH) is a command interface and protocol often used by network administrators to connect securely to a remote computer. SSH replaces its non-secure counterpart rsh and rlogin. There are two versions of the protocol, ssh v1 and ssh v2. The AlterPath Console Server offers both.

To open an ssh session to a serial port or the next free serial port from a pool, issue the command:

```
ssh -l <username>:<server> <hostname or IP address>
```

Where: <username> is the user configured to access that serial port. It is present either in the local CAS database or in a Radius/Tacacs/LDAP/Kerberos, etc database.

<Server> can be just the TCP port number assigned for that serial port (7001, 7002, etc), (3000, etc), the alias for the server connected to that serial port.

Using the Command Line Interface (CLI)

<hostname or IP address> is the hostname configured in the workstation where the ssh client will run (through /etc/hosts or DNS table). It can also be just the IP address of the Alterpath ACS (Ethernet's interface) configured by the user or learned from DHCP.

To exit the ssh session, press the hot key configured for that ssh client (usually "~.").

ts_menu Access

To access the serial port (telnet or ssh) using the ts_menu, login to the CAS unit and, after receiving the shell prompt, type in:

```
ts_menu
```

If configured, the menu will display the servername otherwise it defaults to the serial port number. See the sample menu below:

```
Serial Console Server Connection Menu for your Master  
Terminal Server
```

```
1 ttyS1 2 ttyS2 3 ttyS3 4 ttyS4  
5 ttyS5 6 ttyS6 7 ttyS7 8 ttyS8
```

Type 'q' to quit, a valid option[1-8], or anything else to refresh:

Closing the session from ts_menu (from the console of your unit)

1. Enter the escape character.

The escape character is shown when you first connect to the port.

In character/text Mode, the Escape character is ^] (caret and bracket, for telnet) or ~. (tilde and period, for SSH).

After entering the escape character, the following menu is shown:

```
Console escape. Commands are:
```

```
l go to line mode  
c go to character mode
```

Power Management

```
z suspend telnet
b send break
t toggle binary
e exit telnet
```

2. Press “e” to exit from the session and return to the original menu.

Select the exit option and you will return to the shell prompt.

Closing the session from ts_menu

From Telnet

You have to be sure that a different escape character is used for exiting your telnet session; otherwise, if you were to exit from the session created through the `ts_menu`, you will close your entire telnet session to your unit.

To do this, when you first telnet to your unit, use the “-e” option.

Example: to set Ctrl-? as the escape character, type:

```
telnet -e ^? 192.168.160.10
```

To exit from the session created through the `ts_menu`, just follow Step 1 from above. To exit from the entire telnet session to your unit, type the escape character you had set.

From SSH

If you use SSH to make the first connection to the ACS, then the escape character for each session becomes: `~.~.` (tilde, tilde, period)

Power Management

The Power Management forms (**Power Management > Outlets Manager** or **View IPDUs Info**) allows you to manage the power outlets on the Cyclade’s AlterPath PM family of Intelligent Power Distribution Units (IPDUs) or view information about the IPDUs connected to the ACS.

The **Outlets Manager form** is used to power the remote machines on and off, check the status, and lock the power outlet in the on or off state to prevent accidental changes. The **View IPDUs Info form** is used to view information about the status of the IPDU units.

For information on how to configure Power Management, refer to the *Power Management* section of *Chapter 4: Web Manager for Administrators*.



Figure 3-4: Power Management Configuration Form

Security

The Security form allows you to change your password.

▼ **To Change Your Password**

1. From the menu panel, select **Security**.

The system brings up the **Security** form.

Security

The screenshot shows the 'Security' form in the Cyclades Web Manager interface. The interface has a brown and yellow color scheme. At the top left is the 'cyclades' logo. At the top center is the text 'Cyclades Web Manager - Regular User'. At the top right is a 'logout' link and system information: 'Host Name CAS', 'IP Address 10.10.10.35', and 'Model: ACS4'. On the left side, there is a vertical menu with 'Connect', 'Power Management', and 'Security' (which is highlighted). The main content area is a light yellow rectangle containing three text input fields: 'Current Password', 'New Password', and 'Repeat New Password'. Below these fields is an 'OK' button. At the bottom right of the main area is a 'Help' icon.

Figure 3-5: Password Management Form

2. From the **Security** form enter your current password and your new password (twice).
3. Select **OK** when done.
4. Log out and log in using your new password to verify your password change.

Chapter 4

Web Manager for Administrators

This chapter discusses the procedures for configuring ACS using the Web Manager. It is organized as follows:

- Overview
- Logging In
- ACS Web Manager: GUI Elements
- Configuring in Wizard Mode
 - Security Profile
 - Network Settings
 - Port Profile
 - Access
 - data Buffering
 - System Log
- Configuring in Expert Mode
 - Applications
 - Network
 - Security
 - Ports
 - Administration

Overview

This chapter addresses the System Administrator who is responsible for configuring the ACS Web Manager and its users. For information on how to configure ACS using vi or Command Line Interface (CLI), please consult the *ACS Advanced Administration Guide*.

The ACS Web Manager provides two modes of operation: Wizard and Expert. This chapter describes the functionality of the Web Manager in the two modes of operation, and details the menu selections available under each mode. If you are a regular user, refer to *Chapter 3: ACS for Regular Users*.

Logging In

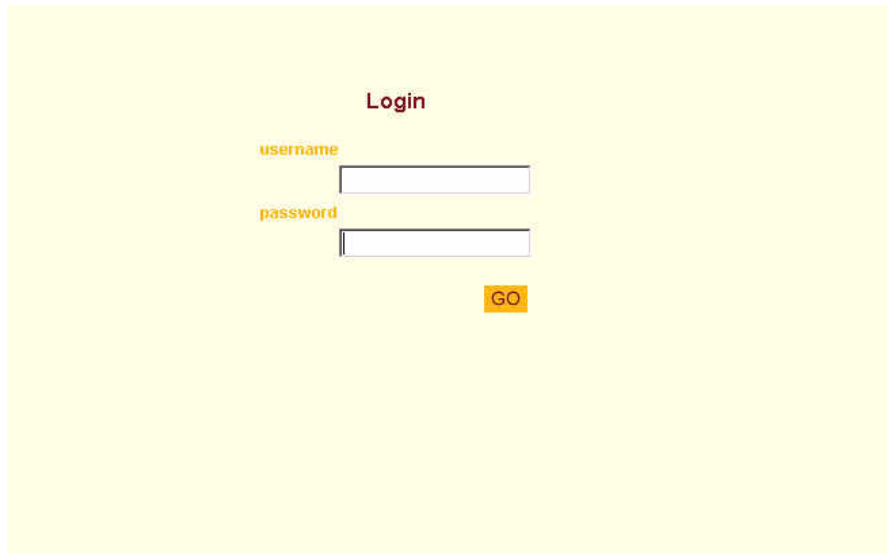
1. Connect your internet browser to the Console Server by typing in the Console Access Server's IP address (*e.g.*, `http://10.0.0.0`) in the browser's address (URL) field.

Note: To determine the IP address of the ACS, switch on the ACS connected to the Ethernet where there is a DHCP server. When you inquire, based on the MAC address (the 12-digit hexadecimal number located at the bottom of the ACS unit), the server will provide the appropriate IP address. If there is no DHCP server, use the default static IP address that is pre-configured in the ACS: 192.168.160.10.

For more detailed information, see Chapter 2: Installing the ACS.

The system brings up the ACS Login page:

Logging In



The screenshot shows a login page with the title "Login" centered at the top. Below the title, there are two input fields. The first field is labeled "username" and the second is labeled "password". To the right of the password field is a yellow button with the text "GO" in black.

Figure 4-1: Login page

2. Log in as “**root**” and type in the root password. The default password is “**tslinux**”.

Warning: If you have performed the network configuration steps described in Chapter 2, you may have already changed the default password. If you have not, make sure you do so after login.

After login, if another administrator is logged in to the Web Manager, the following dialog box appears, otherwise, the ACS **Ports Status** page will appear.

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

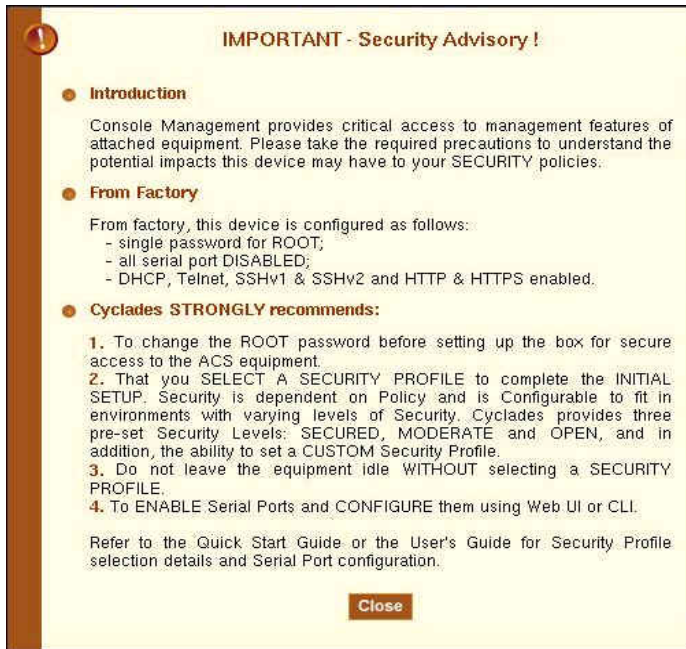
- Proceed. Log into the device and log-off the currently logged-in administrator.
- Cancel.

Apply

3. Click on the appropriate radio button and then click on the **Apply** button.

Note: Take note of this login procedure. All subsequent online procedures in this chapter assume that you are already logged in.

Note: The following Security Advisory appears the first time ACS unit is accessed. Note that the browser's pop-up blocker should be disabled for this dialog box to appear.



ACS Web Manager: Elements

The ACS Web Manager operates in two modes:

- Wizard
- Expert

Wizard Mode

The wizard is designed to simplify configuring the ACS for the administrator. It is designed to perform the necessary set up and configuration quickly.

When you log in to ACS, by default the system brings up the Expert Mode. To change to the Wizard Mode, click on the button located in the left bottom corner of the screen labeled **Wizard**.



Figure 4-2: Security Profile Setup

Shown above is a typical page of the ACS web interface in Wizard Mode. The user entry panel or form varies depending on the selected menu item. The ACS uses forms and dialog boxes (*i.e.*, pop-up windows that prompt you for an answer or command) for data entry.

Expert Mode

Designed for advanced users, this is the default mode when you log in to the ACS. If you are in the **Wizard** mode, you can change to this mode by clicking on the **Expert** button at the bottom of the menu panel.

Shown below is a typical ACS screen in Expert Mode. The main difference between the two modes is the addition of a top menu bar in the Expert Mode to support more detailed and customized configuration.

In Expert mode the top menu bar contains the primary commands, and the left menu panel contains the secondary commands. Based on what you select from the top menu bar, the left menu selections will change accordingly.

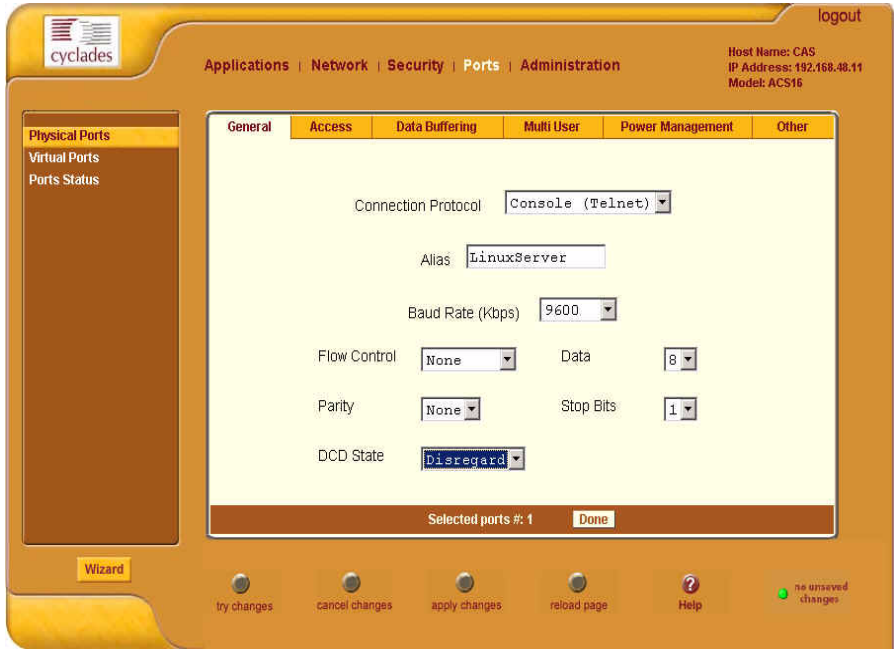


Figure 4-3: Serial Ports Setup

Occasionally, an Expert Mode menu selection will comprise multiple forms (such as the one shown above). These forms are identified by their tabs. Select the tab to access the desired form.

Button Functions

The control buttons located on the bottom of the ACS Web Manager window provides you the following functions for operating the interface.

Table 4-1: Web Manager Buttons

Button Name	Use
Wizard / Expert	Switches the ACS Web Manager screen to either Expert or Wizard Mode. The Expert Mode is the default mode. Clicking the Expert mode will change the screen Wizard mode.

Table 4-1: Web Manager Buttons

Button Name	Use
Help?	Invokes the Help window which provides brief description of the functionality behind the active form.
Back (Wizard Mode)	Goes back to the previous form (<i>i.e.</i> , the form preceding the current form as it appears in the menu).
Next (Wizard Mode)	Goes to the next form (<i>i.e.</i> , the form succeeding the current form as it appears in the menu).
Try Changes	Test or run the system based on the settings from the current form without having to save the configuration.
Cancel Changes	Cancel your changes or revert back to the original configuration parameters.
apply changes	Save your changes to the ACS Flash card.
Reload Page (Expert Mode)	Refreshed the active page

Saving Your Configuration

The **Unsaved Changes** indicator on the lower right hand corner of the Web Manager window reminds you that a configuration parameter has changed, and it requires to be saved.



Figure 4-4: Configuration parameters unsaved indicator

Unless you do not need to save your configuration, be sure to select the **apply changes** button to ensure that your changes are saved to Flash.

Configuring the ACS in Wizard Mode

The Wizard Mode configuration is comprised of six steps:

- “Security Profile” on page 38
- “Network Settings” on page 38
- “Port Profile” on page 43
- “Access” on page 45
- “Data Buffering” on page 49
- “System Log” on page 52

Security Profile

A Security Profile consists of a set of parameters that can be set to control access to the ACS. The ACS offers three pre-defined security profiles, **Secured**, **Moderate**, **Open**, and an option to configure a **Custom** profile. A fifth option, **Default** sets the parameters to the same as **Moderate**.

Note: The first step in configuring AlterPath ACS is to define a Security Profile.



Figure 4-5: Security Profile Setup form

Configuring the ACS in Wizard Mode

The following tables illustrate the properties for each of the Security Profiles. The enabled services in each profile is designated with a check mark. Note that the **Default** option will set the parameters to the same as **Moderate**, and the **Custom Profile** allows for individual configurations.

Table 4-2: Enabled services to access the ACS box for each security profile.

Access to ACS	Secured	Moderate	Open	Default	Custom
Telnet		✓	✓	✓	Individually Configurable
SSH v1		✓	✓	✓	
SSH v2	✓	✓	✓	✓	
Allow SSH root access					
HTTP		✓	✓	✓	
HTTPS	✓	✓	✓	✓	
HTTP redirection to HTTPS		✓	✓	✓	

Table 4-3: Enabled services to access the serial ports for each profile.

Access to Serial Ports	Secured	Moderate	Open	Default	Custom
SSH to Serial Ports	✓	✓	✓	✓	Individually Configurable
Telnet to Serial Ports		✓	✓	✓	
Raw Connection to Serial Ports		✓	✓	✓	
Serial Port Authentication	✓				

Table 4-4: Enabled protocols for each profile shown with a check mark.

Other Services	Secured	Moderate	Open	Default	Custom
SNMP			✓		Individually Configurable
RPC			✓		
ICMP		✓	✓	✓	
FTP					
IPSec					

▼ **To Configure the Security Settings**

1. Select **Step 1: Security Profile**
2. Select a pre-defined Security Profile, or create a Custom Profile.
3. Select **apply changes** to save the configuration to Flash.

Note: Before proceeding forward to Network Settings, the following dialog box appears. The protocols and access methods for the Serial Ports must match the selected Security Profile. To configure parameters for all Serial Ports, see “Port Profile” on page 43. To modify services for each Serial Port, see “Physical Ports” on page 106



Network Settings

The network settings form allows configuring parameters to make ACS accessible over the network.

▼ *To configure the Network Settings*

1. Select **Step 2: Network Settings**.

The system brings up the DHCP page (shown below). By default, **DHCP** is active, which means that the system is configured to use the DHCP server.



Figure 4-6: Network Parameters with DHCP enabled

2. If you are using DHCP, proceed to **Step 3: Port Profile**; if not, click on the checkbox to deselect DHCP and enter your network settings manually. The Network Settings entry fields should appear as follows:

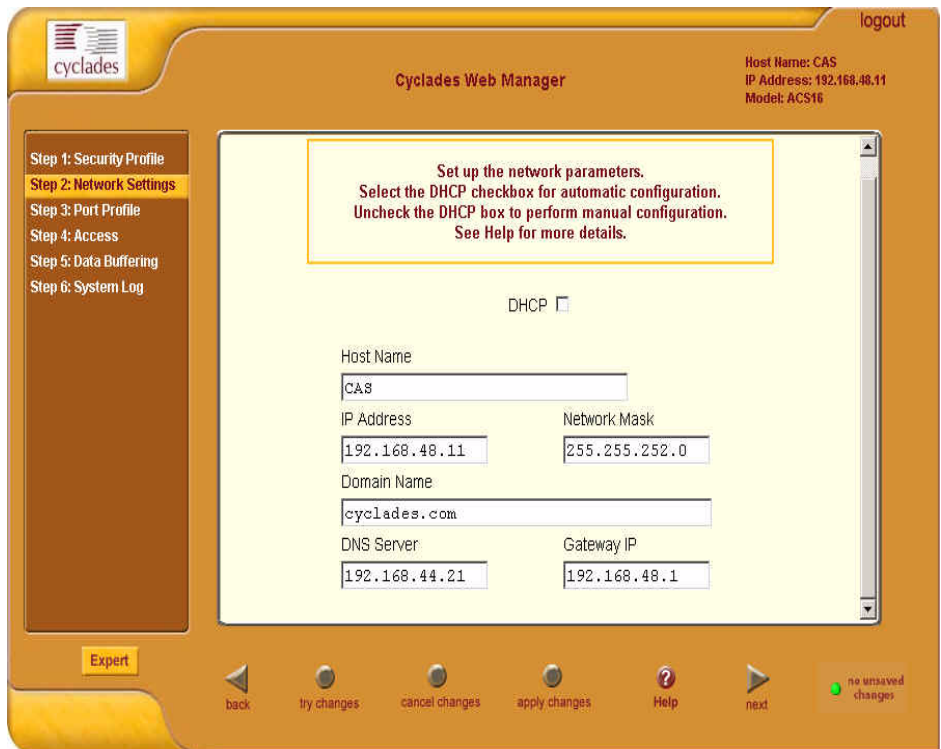


Figure 4-7: Network Parameters with DHCP disabled

3. Enter the network information:

- Host Name
- IP addresses
- Network Mask
- Domain Name
- DNS Server
- Gateway IP

4. Select **apply changes** to save configuration to Flash.

5. Select the **Next** button OR proceed to **Step 3: Port Profile** section.

Port Profile

The Port Profile configures your Console Access Profile (CAS), defining the protocol and type of command line interface you will use to access the ACS. The Port Profile controls the speed, data size, parity, and stop bits of all ports.

It sets the flow control to hardware, software, or none; and sets the DCD signal and tty after the system establishes a socket connection to that serial port.

Note: In **Wizard** mode the system assumes that all devices will be connected with the same parameter values. If you need to assign different parameters for each device, then you must click on the **Expert** mode button and select **Ports** > **Physical Ports** to enter these values. By default all Serial Ports are disabled. The administrator can select and assign specific users to individual ports through the Expert mode.

▼ To Set Parameters for All Serial Ports

1. Select Step 3: Port Profile

The system displays the Port Profile form

The screenshot shows the Cyclades Web Manager interface. On the left is a navigation menu with steps: Step 1: Security Profile, Step 2: Network Settings, Step 3: Port Profile (highlighted), Step 4: Access, Step 5: Data Buffering, and Step 6: System Log. Below the menu is an 'Expert' button. The main content area has a yellow header with the text: 'Set up the CAS (Console Access Server) profile, for the serial ports. Specify the serial parameters for all ports. See Help for more details. The previous port-specific parameters will be discarded.' Below this is a form with the following fields: Connection Protocol (dropdown: Console (SSH)), Baud Rate (dropdown: 9600), Flow Control (dropdown: None), Data Size (dropdown: 8), Parity (dropdown: None), Stop Bits (dropdown: 1), and Authentication Required (checkbox, unchecked). At the bottom of the form are navigation buttons: back, try changes, cancel changes, apply changes, Help, next, and a red 'unsaved changes' indicator.

Figure 4-8: Serial Ports Parameters (Setup for All Serial Ports)

2. From the Port Profile form, complete the necessary fields.

Table 4-5: Serial Ports Parameters

Field Name	Definition
Connection Protocol	The method you will use to access the serial ports. Cyclades recommend SSH to ensure that all data and authentication information are encrypted. Other options are Telnet and Raw Data (for un-negotiated plain socket connections).
Flow Control	The method of flow control used by the attached devices (Hardware, Software, or None).
Baud Rate	The serial speed on each console port, which should match the equipment you will connect to. The recommended Baud Rate is 9600.
Data Size	Number of data bits used by the attached devices (5, 6, 7 or 8).
Parity	Parity used by the attached devices (None, Odd, or Even).
Stop Bits	Number of stop bits used by the attached devices.
Authentication Required	Selecting this checkbox sets the system to require authentication to access the ports. This is done in the local database in the ACS.

Note: *If you require individual Serial Port Authentication, then you must add users through Wizard **Step 4: Access**.*

3. Select **apply changes** to save configuration to Flash.
4. Select the **Next** button or proceed to the next section, **Step 4: Access**.

Access

Configure which users are allowed access to the ports. By default any user can access any port as long as they have a valid user ID and password.

Note: To grant users access to specific ports, switch to the *Expert Mode*, then go to *Security > Users and Groups*.

From this window, you can:

Change a User Password

- Add a user
- Delete a user

▼ To Configure User Access to Serial Ports

1. Select **Step 4: Access**.

The system brings up the Access screen:



Figure 4-9: User Access Setup

2. To complete your User Access configuration, proceed to the appropriate subheadings of this section: *Changing a User Password*, *Adding a User*, or *Deleting a User*.

▼ **To Change a User Password**

Note: *If you haven't changed your root administration password, now is the time to change it using the **Change User Password** dialog box.*

1. From the **Users** scrollable field box of the Access window, select the user whose password you want to change, and then click the **Change Password** button.

The system brings up the **Change User Password** dialog box:



Figure 4-10: Password Change Dialog box

2. Type in the new password in the two entry fields of the dialog box, and then click on the **OK** button.

▼ **To Add a User**

1. If you haven't opened the Access form, select **Step 4: Access** from the menu panel.

The system brings up the Access form.

2. From the Access form, select the **Add** button.

The system brings up the **Add User** dialog box:

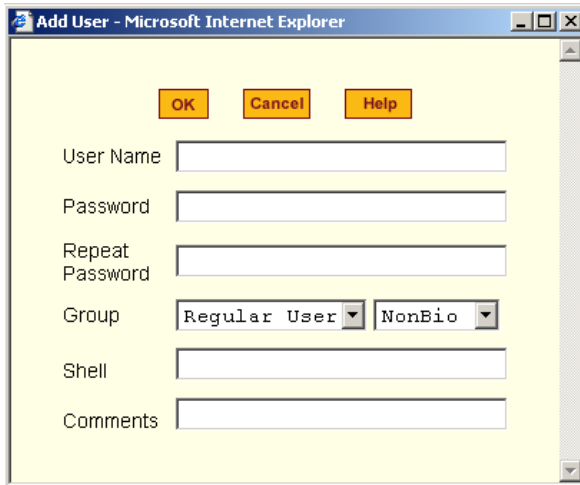


Figure 4-11: Add User Dialog Box

3. Enter the necessary User information into the following fields:

Table 4-6: Add User fields

Field Name	Definition
User Name	Name of the ACS user.
Password	Password to be used by the user to access ACS.
Repeat Password	Re-type the password.
Group	Select the user group to which the user belongs. There are two default groups with the following associated access rights: Admin (Read/Write) Regular User (Read Only)
[dropdown list]	Select whether the user of this group is a NonBio or a BioUser. The NonBio group, is the correct choice for regular users. The BioUser group should only be selected if authentication will be made through the Cyclades AlterPath Bio (biometric authentication).

Table 4-6: Add User fields

Field Name	Definition
Shell	Text string you wish to use as part of the shell prompt for the current user.
Comments	Comments about the current user.

Note: To define a new group, select the *Expert* button to switch to the *Expert Mode*, and then select *Security > Users and Groups*.

4. Select the **OK** button when done.
5. From the bottom of the main window, select the **apply changes** button.

▼ **To Delete a User**

1. From the **Users** scrollable field box of the Access form, select the user that you wish to delete.
2. Select the **Delete** button.
3. Select **apply changes**.

For information on how to configure users and groups, see *Users and Groups* under configuring ACS in expert mode.

Data Buffering

This step configures the data buffering file and mode for all ports that ACS controls.

You can set data buffering to be done in local files or in remote files through NFS. When using remote files, the remote server's disk/partition space imposes a limitation and the data is kept in linear (or sequential) files in the remote Server. When using local files, the size of the available RAMdisk also imposes a limitation. You can have data buffering done in file, syslog or both.

If you accept the default configuration values for data buffering, skip this step and proceed to **Step 6: System Log**. Do not click on the **Enable Data Buffering** checkbox.

▼ To Configure Data Buffering

1. Select **Step 5: Data Buffering**.

The system brings up the Data Buffering form:

The screenshot shows the Cyclades Web Manager interface. On the left is a sidebar with a list of steps: Step 1: Security Profile, Step 2: Network Settings, Step 3: Port Profile, Step 4: Access, Step 5: Data Buffering (highlighted), and Step 6: System Log. The main area is titled 'Cyclades Web Manager' and shows a 'Data Buffering' configuration form. A yellow warning box at the top of the form states: 'Set up data buffering to the output from the consoles in a console log file. See Help for more details. The previous port-specific parameters will be discarded.' Below the warning, the form includes: 'Enable Data Buffering' checkbox (checked), 'Destination' dropdown menu (set to 'Local'), 'Mode' dropdown menu (set to 'Circular') and 'File Size (Bytes)' text input (set to '100'), 'Record the timestamp in the data buffering file' checkbox (unchecked), and 'Show Menu' dropdown menu (set to 'Show all options'). At the bottom of the form are navigation buttons: 'back', 'try changes', 'cancel changes', 'apply changes', 'Help', 'next', and a 'unsaved changes' indicator.

Figure 4-12:Data Buffering Form

2. Select the **Enable Data Buffering** checkbox, if unselected.

The system invokes the Data Buffering input fields.

3. Complete the input fields as follows:

Table 4-7: Data Buffering fields

Field Name	Definition
Destination	Destination of the buffer files: Local (<i>i.e.</i> , Ramdisk) or Remote.

Table 4-7: Data Buffering fields

Field Name	Definition
Mode	If you selected Local destination, choose the file sort mode. Select Linear for sequential files, Circular for non-sequential files.
File Size (Bytes)	If you selected Local destination, the value for this field cannot be zero.
Record the time stamp...	Commands the system to include a time stamp in the buffer.
Data Buffering file	Name of the buffer file.
Show Menu	Defines what you want to show in the menu of the buffer file. Select from: Show all options, No, Show data buffering file only, and Show without the erase options.

- If you selected **Remote** from the Destination field, type in the **NFS File Path** from the resulting form (i.e., specify the NFS mount point. The NFS server must be already configured, and the mount point exported):

Set up data buffering file and mode for ports controlled by the ACS4

Enable Data Buffering

Destination:

NFS File Path:

Record the timestamp in the data buffering file:

Show Menu:

- Click on the **apply changes** button.

The system can filter messages based on their content and perform an action (e.g. to send an e-mail or pager message). To configure data buffering to send

a notification alarm, you must use the **Notifications** form (Go to Expert Mode: **Administration** > **Notifications**).

System Log

The System Log form allows you to configure one or more syslog servers to receive syslog messages that are generated by the ACS. The ACS sends syslog messages to all syslog servers that are defined here.

Note: To configure syslog with data buffering features for specific ports, switch to the Expert Mode, and then go to **Ports** > **Physical Ports** > **Data Buffering**.

▼ To Configure Syslog servers

1. Select Step 6: System Log.

The system brings up the System Log form:



Figure 4-13: Syslog Form

2. From the System Log form, select the Syslog facility number that the ACS will use to send out syslog messages.

Configuring the ACS in Expert Mode

3. To add a new syslog server, type in the IP address in the **New Syslog Server** field, and click **Add**. (Repeat step for as many syslog servers you need to add.)

OR

4. To delete a syslog server, select the **Syslog** server to be deleted from the **Syslog Servers** scrollable list box, and then click **Delete**.
5. Click on the **apply changes** button at the bottom of the main panel.

Configuring the ACS in Expert Mode

This section presents the procedures for configuring the ACS Web Manager in Expert Mode. This mode is designed for the advanced user administrator who needs to configure the ACS beyond the capabilities of the basic wizard mode.

As indicated in the top menu bar, there are five additional areas of ACS configuration in Expert mode:

- “Applications” on page 56
- “Network” on page 67
- “Security” on page 99
- “Ports” on page 106
- “Administration” on page 125

Expert Mode Menu

Each top menu option provides additional side menu selections. Their functions are as follows:

Table 4-8: Applications Menu

Menu Selection	Use this menu to:
Connect	Select and connect to a port.
Power Management	View and edit IPDU settings. This menu comprises five tabbed forms: Outlets Manager, View IPDUs Info, Users Manager, Configuration, and Software Upgrade.

Table 4-8: Applications Menu

Menu Selection	Use this menu to:
Terminal Profile Menu	Create command menu for a terminal (i.e., CLI or VI).

Note: *Most of the fields for each form are defined in the procedure. For a more detailed definition of these field names or terms refer to the Glossary of this manual.*

Table 4-9: Network Menu

Menu Selection	Use this menu 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	Enable the insertion or ejection of PCMCIA cards; configure the type of access and connection (e.g., Modem, ISDN, Ethernet) to ACS.
VPN Connections	Configure IPsec tunnels to establish a secure connection between ACS and a security gateway machine.
SNMP Daemon Settings	Configure the SNMP server to manage complex networks.
Firewall Configuration	Configure static IP tables
Host Table	View table of hosts; create, edit, and delete hosts.
Static Routes	View, create and delete routes from the table.

Table 4-10: Security Menu

Menu Selection	Use this menu to:
Users and Groups	Create/edit users and groups, establish/change their passwords, access rights and privileges.
Active Port Sessions	View the status of all active port sessions.
Security Profile	Select a pre-defined Security Profile or configure a Customer Profile.

Table 4-11: Ports Menu

Menu Selection	Use this menu to:
Physical Ports	Modify ports settings for individual or all ports. Physical Ports is composed of five configuration forms as identified by their tab names: General, Access, Data Buffering, Multi-User, Power Management and Other .
Virtual Ports	Add, edit or delete port slaves.
Port Status	Shows the current status of each port. The information provided here are: RS232 Signal Status and user connected to each port.

Table 4-12: Administration Menu

Menu Selection	Use this menu to:
System Information	View summary information about the system (<i>e.g.</i> , Kernel, CPU, memory, <i>etc.</i>).
Notifications	Configure the system to deliver alarm notification by email, pager, or snmp trap; define alarm triggers; set data buffering to send notification.
Time/Date	Set the unit's date and time.
Boot Configuration	Defines the settings for loading the operating system in the event that the ACS fails to boot successfully.

Table 4-12: Administration Menu

Menu Selection	Use this menu to:
Backup Configuration	Use a FTP server to save and retrieve your ACS configuration; use a storage device to store your configuration.
Upgrade Firmware	Upload/upgrade new firmware.
Reboot	Reboot the ACS system.

Applications

Connect

The **Connect** form, which launches a Java browser, is used to:

- Connect to the ACS box. The connection type is always SSHv2.
 - Connect to a console port based on which port you select from the drop down menu. The connection type depends on how your ACS is configured.
1. From the top menu bar, select **Applications**; from the left menu panel, select **Connect**.

The system invokes the port selection form:

Configuring the ACS in Expert Mode

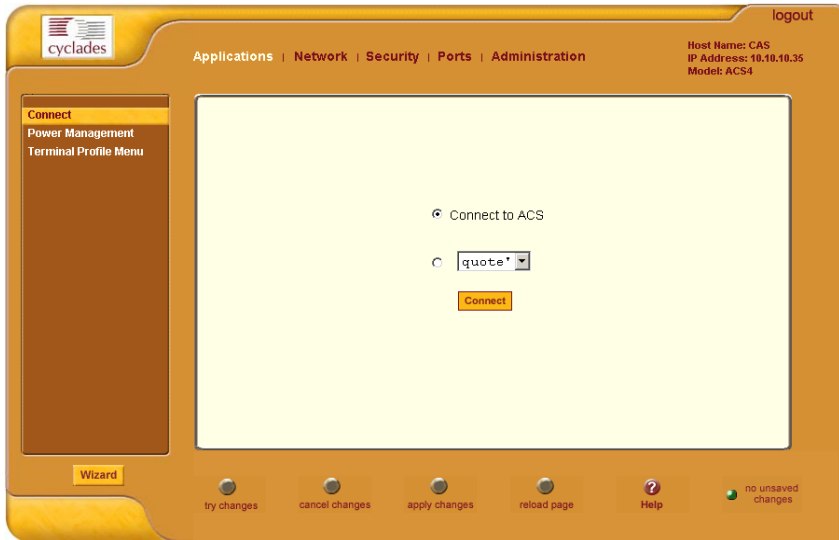


Figure 4-14: ACS and Serial Ports Connection Form

2. To connect to a port (by default, the radio button is selected for connecting to a port), select the port from the drop down menu to which you wish to connect, and then click on **Connect**.

- OR -

To connect to the ACS box, select the radio button for **Connect to ACS**, and click on **Connect**.

Depending on your selection, the system either opens a Java connection to the port selected, or launches SSHv2 connection to the ACS box.

Power Management

ACS allows you to remotely manage all Intelligent Power Distribution Units (IPDUs) connected to the ACS. Power management configuration comprises five tabbed forms:

Table 4-13: Power Management Tabs

Form Title	Use
Outlets Manager	Switch on/off and lock/unlock outlets.

Table 4-13: Power Management Tabs

Form Title	Use
View IPDUs Info	View IPDU information by ports and slaves. The information form provides real-time, global, current monitoring of all connected devices.
Users Manager	Add or delete users assigned to specific outlets.
Configuration	Enable over power protection, syslog and alarm notification from any specified port. The form allows you to set a current alarm threshold that once exceeded will have the ACS sound an alarm or send a notification message.
Software Upgrade	Upgrade power management software.

You can configure the port assignments of the IPDU units, including the user and group access using the Power Management form of the Ports menu (**Ports > Physical Ports > Power Management**).

Outlets Manager

The **Outlets Manager** form allows you to check the status of all IPDUs connected to the Console Server, including their outlets. Any user who has Administrative privileges can turn on, turn off, cycle, lock and unlock the outlets.

1. From the top menu bar, select **Applications**; from the left menu panel, select **Power Management**.

The system invokes the following form:

Configuring the ACS in Expert Mode

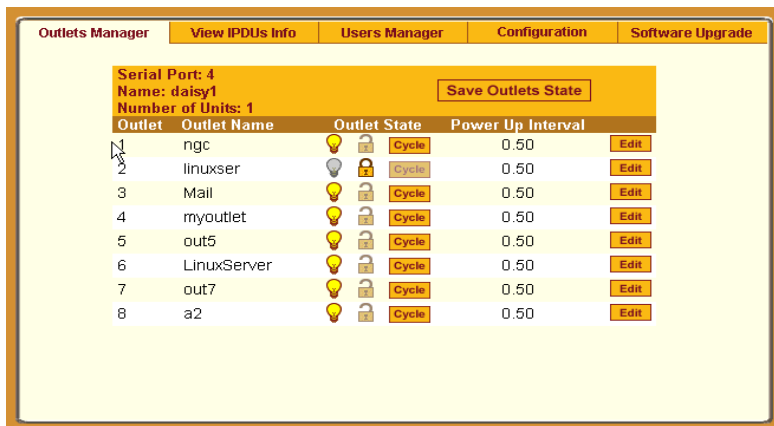


Figure 4-15: Power Management Form

In the example above, the yellow bulbs (*i.e.*, the actual color online when the switch is ON) and the opened padlock indicate that the outlets are switched on and unlocked.

2. To switch on/off an outlet, click on the light bulb; to lock/unlock an outlet, click on the padlock.

In the sample form below, outlet 2 is switched off and locked



3. To save your changes, click on the **Save Outlets State** button located in the form.
4. From the lower control buttons of the main window, click on the **apply changes** button.

To Edit the Power Up Interval

You can edit the power up interval of an outlet as follows:

1. From the **Outlets Manager** form (**Applications > Power Management**), select the particular outlet that you wish to edit by clicking the adjacent **Edit** button.

The system brings up the **Edit Outlet** dialog box:

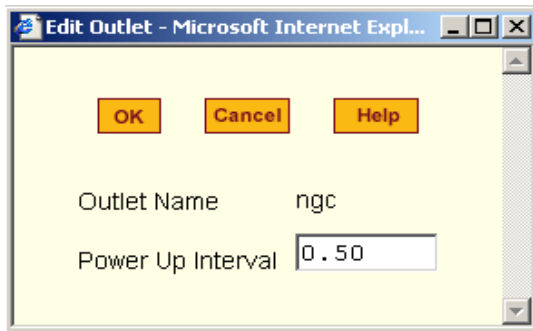


Figure 4-16: Edit Outlet Dialog Box

2. From the **Power Up Interval** field of the Edit Outlet dialog box, enter the time interval (in seconds) in which the system waits after the outlet is switched on; select **OK** when done.

View IPDUs Info

The IPDU Info form allows you to view all IPDU information (*e.g.*, number of outlets of each unit, current, temperature, alarm threshold levels, firmware, etc.) by serial port.

The form stores historical values of the maximum current and the maximum temperature.

To view IPDU information, perform the following steps:

1. From the top menu bar, select **Applications**; from the left menu panel, select **Power Management**; from the form tabs, select **View IPDUs Info**.

2. The system brings up the **IPDUs Info** form:

The screenshot shows a web interface with a top navigation bar containing five tabs: "Outlets Manager", "View IPDUs Info", "Users Manager", "Configuration", and "Software Upgrade". The "View IPDUs Info" tab is active. Below the tabs, there is a section titled "Serial Port 4: General Information" with two buttons: "Clear Max Detected Current" and "Clear Max Detected Temperature". The information displayed includes: Name: PowerMgm-4, Syslog: ON, Number of Outlets: 8, Number of Units: 1, Buzzer: ON, Over Current Protection: OFF. Below this is a section titled "Master Unit Information:" with the following details: Model: PMB 15A, Software Version: 1.2.0, Alarm Threshold: 15.0A, Current: 0.0A, Maximum Detected: 0.4A, and Temperature: Maximum Detected:.

Figure 4-17:Power Management Information Screen

3. To delete the stored values for the maximum detected current, select the **Clear Max Detected Current** button.
4. To delete the stored values for the maximum detected temperature, select the **Clear Max Detected Temperature** button.

Users Manager

The Users Management form of Power Management allows you to assign users to selected outlets for each serial port, and vice versa.

To add a user or edit an assigned user, perform the following steps:

1. From the top menu bar, select **Applications**; from the left menu panel, select **Power Management**; from the tabs, select **Users Manager**.

The system brings up the **Users Manager** form:

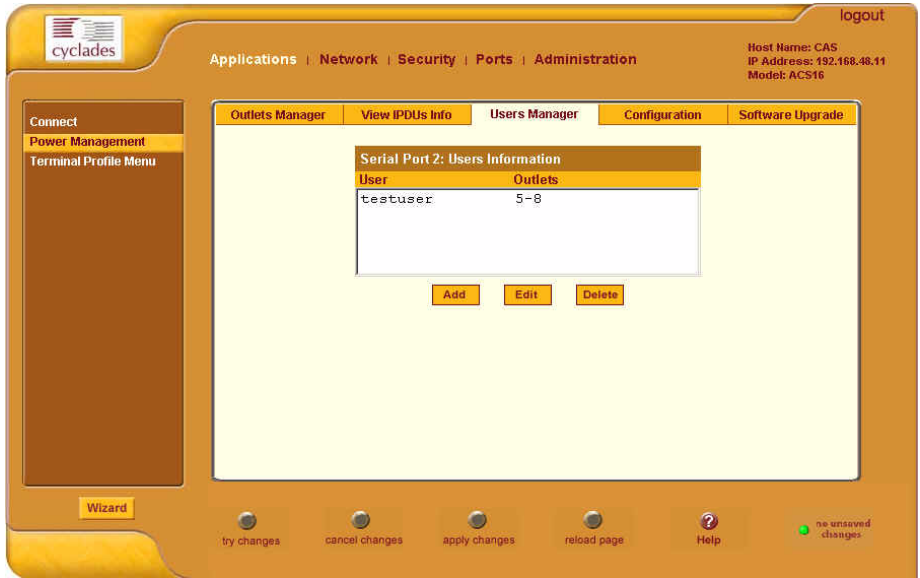


Figure 4-18:Power Management Users Manager Form

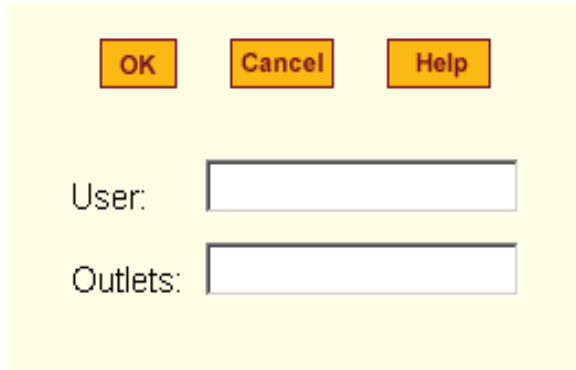
2. To edit an assigned user, select the user you wish to edit from the Serial Port view table and then select the **Edit** button that corresponds to the table.

- OR -

To add or assign a new user select the **Add** button from the appropriate Serial Port view table.

The system brings up the **Add/Edit User** dialog box:

Configuring the ACS in Expert Mode



3. From the **Add/Edit User** dialog box, modify or enter in the corresponding fields the user and the outlets to which the user is assigned, and then select the **OK** button.

Note: In the **Outlets** field, use the comma to separate each outlet; use the hyphen to indicate a range of outlets (e.g., **1, 3, 6, 9-12**). Selecting **Edit** will not allow you to edit or delete the user, only the outlet assignments for that user.

4. Verify your entry by checking the appropriate Serial Port table from the Users Manager form.
5. Select the **apply changes** button located at the bottom of the ACS application window to save your configuration.

To Delete a User

1. To delete an assigned user, select the user you wish to delete from the appropriate Serial Port view table.
2. Based on the Serial Port view table that you are working on, select the corresponding **Delete** button.
3. Select the **apply changes** button located at the bottom of the ACS application window.

Configuration

To configure IPDUs to generate alarms or syslog files, perform the following steps:

1. From the top menu bar, select **Applications**; from the left menu panel, select **Power Management**; from the default Outlets Manager form select the **Configuration** tab.

The system brings up the Configuration form:

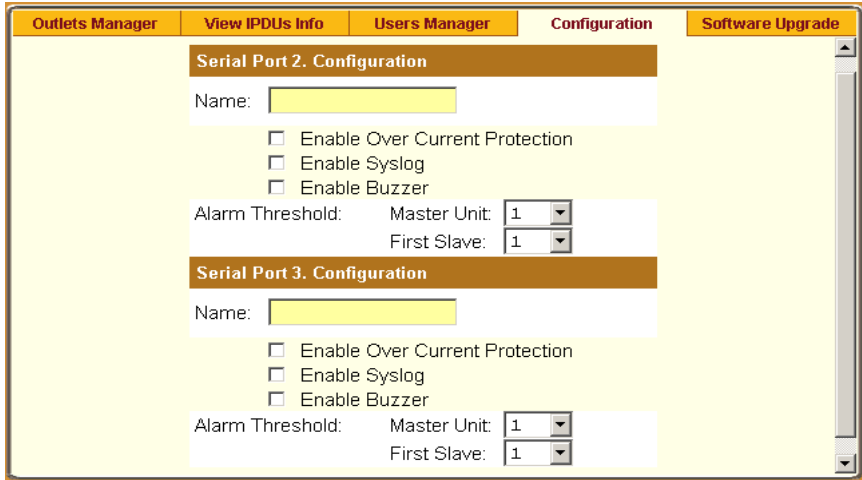


Figure 4-19:Power Management Configuration Form

2. From the Configuration form, select the Serial Port you wish to configure and then click on the appropriate radio buttons to enable/disable Over Current Protection, Syslog, and Buzzer.
3. If enabling the buzzer or alarm notification, provide the Alarm Threshold (1-100 amps) for that master or slave unit.
4. Click on the **apply changes** button at the bottom of the ACS application window.

Software Upgrade

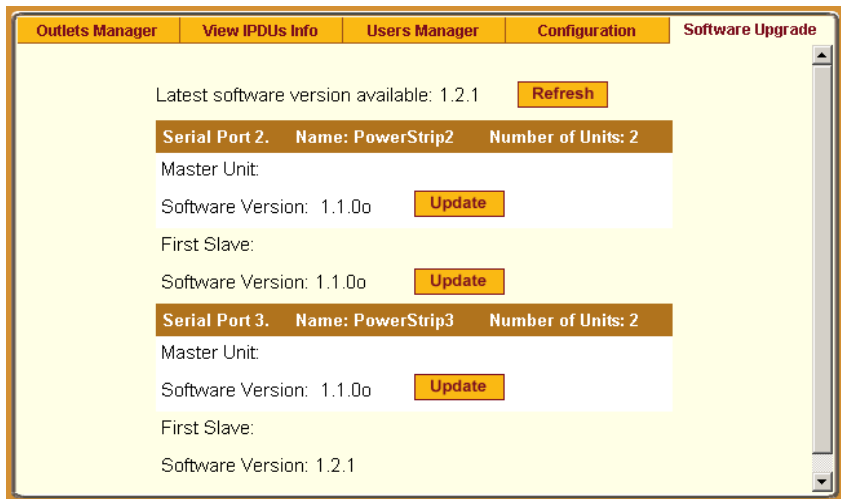
The **Software Upgrade** form of Power Management allows you to upgrade the Power Management software for a selected serial port. The first line of the form shows the **latest software version available**. The presence of an Upgrade button indicates that a new software version for that master or slave port is available.

To upgrade the software for a selected port, perform the following steps:

Configuring the ACS in Expert Mode

1. Go to the Cyclades web site and enter the “Download/Drivers” area. Download the latest AlterPath PM firmware to the /tmp folder in the ACS box. Be sure to name the firmware “*pmfirmware*” otherwise the ACS should not detect it. Note that you cannot copy the firmware image to the ACS unit through the web interface; you must do it via SSH or by accessing the console port.
2. From the top menu bar, select **Applications**; from the left menu panel, select **Power Management**; from the tabs, select **Software Upgrade**.

The system brings up the **Software Upgrade** form:



The screenshot displays the 'Software Upgrade' tab within a web interface. At the top, there are navigation tabs: 'Outlets Manager', 'View IPDUs Info', 'Users Manager', 'Configuration', and 'Software Upgrade'. Below the tabs, the text reads 'Latest software version available: 1.2.1' with a 'Refresh' button to its right. The main content area is divided into two sections, each representing a serial port. The first section is for 'Serial Port 2' (Name: PowerStrip2, Number of Units: 2). It lists 'Master Unit' and 'First Slave', both with a 'Software Version: 1.1.0o' and an 'Update' button. The second section is for 'Serial Port 3' (Name: PowerStrip3, Number of Units: 2). It lists 'Master Unit' with a 'Software Version: 1.1.0o' and an 'Update' button, and 'First Slave' with a 'Software Version: 1.2.1'.

Figure 4-20:Power Management Software Upgrade Form

3. Select the **Refresh** button to ensure that all software information on the form is up-to-date.
4. From the Software Version list, select the software you wish to update, and then select the **Update** button to the right of the listed version.
5. Select the **apply changes** button at the bottom of the configuration window to save your configuration.

Terminal Profile Menu

The Terminal Profile Menu form enables you to create a menu of commands for users to use whenever ACS is used as a terminal server with dumb

terminals attached. The menu should appear when users turn on the dumb terminal and login to ACS.

You can create any valid command recognized by the ACS operating system. The most common use of this feature is to launch an SSH session to a host system.

1. From the top menu bar, select **Applications**; from the menu panel, select **Terminal Profile Menu**.

The system invokes the Terminal Profile Menu form:

The screenshot shows the ACS web interface with the Terminal Profile Menu form. The interface has a top navigation bar with 'Applications | Network | Security | Ports | Administration' and a 'logout' link. The left sidebar contains 'Connect', 'Power Management', and 'Terminal Profile Menu' (which is highlighted). The main content area has a 'Menu title' input field and a 'Menu Options' section containing a table with two columns: 'Action Name' and 'Action/Command'. Below the table are buttons for 'Edit', 'Delete', 'Add', 'Up', and 'Down'. At the bottom of the interface, there are several status indicators: 'try changes', 'cancel changes', 'apply changes', 'reload page', 'Help', and 'no unsaved changes'.

Figure 4-21: Terminal Profile Form

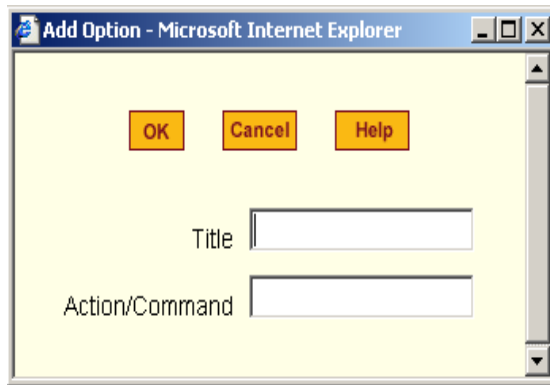
2. To edit a menu option, select the action name from the table and then click on the **Edit** button.

- OR -

To add a new menu option to an existing menu, click on the **Add** button.

Configuring the ACS in Expert Mode

The system invokes the following dialog box:



3. Type in the menu title and/or action to the corresponding entry fields.
4. Verify your entry or edits from the Menu Options list of the Terminal Profile Menu form.
5. To enter or edit another command, repeat steps 2 through 4.
6. Click on the **apply changes** button located at the bottom of the configuration window.

Network

The Network menu allows configuring the ACS' generic network setting as well as additional parameters as described and illustrated in each section below.

The following are the available options:

- Host Settings
- Syslog
- PCMCIA Management
- VPN Connections
- SNMP Daemon Settings
- Firewall Configuration
- Host Table
- Static Routes

Host Settings

The Host Settings form allows you to configure the network settings for ACS.

▼ To Configure Host Settings

1. Select **Network > Host Settings**

The system brings up the **Host Settings** form.

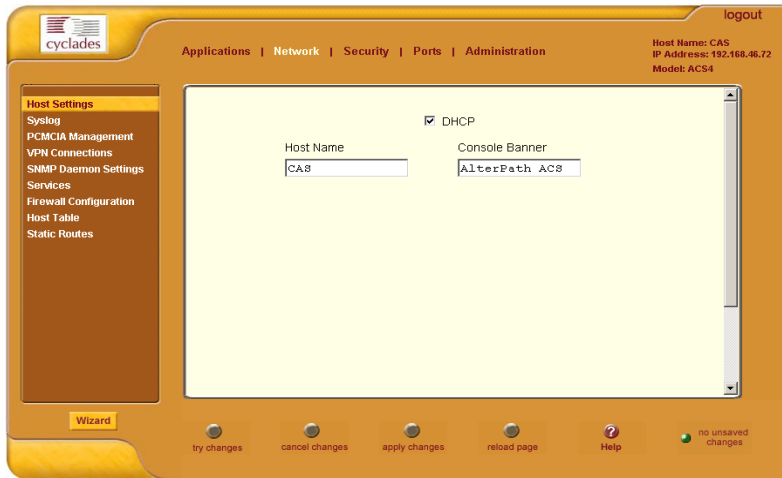


Figure 4-22: Network Host Settings Form with DHCP enabled

By default, the DHCP field checkbox is checked.

2. To disable DHCP and enter the host settings manually, clear the DHCP checkbox.

The system should add the following fields to your form.

Configuring the ACS in Expert Mode

DHCP

Host Name: cyclades

Console Banner: AlterPath ACS

Ethernet Port

Primary IP: 192.168.48.11

Network Mask: 255.255.252.0

Secondary IP: [Empty]

Secondary Network Mask: [Empty]

MTU: 1500

DNS Service

Primary DNS Server: 192.168.44.21

Secondary DNS Server: [Empty]

Domain Name: cyclades.com

Gateway IP: 192.168.48.1

Bonding

Enabled

Figure 4-23: Network Host Settings form with DHCP disabled.

3. On the Host Settings form, complete or edit the following fields:

Table 4-14: Host Settings Fields

Filed Name	Field 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.
Primary IP	IP address of the unit.

Table 4-14: Host Settings Fields

Filed Name	Field Definition
Secondary IP	The second IP address of the unit. Configuring the second IP address, the unit will be available for more than one network.
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 Network Mask	Optional.
MTU	Maximum Transmission Unit used by the TCP protocol.
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	As indicated.
Bonding	Enables redundancy for the Ethernet devices, using the standard Ethernet interface as the primary mode of access and one PCMCIA card as a secondary mode of access. If enabled, the following values should be set:
Miimon	Configure the interval, in milliseconds, in which the active interface is checked to see if it is still communicating.
Updelay	Configure the time, in milliseconds, that the system will wait to make the primary interface active after it has been detected as up.

Caution: If you have set IP Filtering rules before bonding is activated, the interface reference in the firewall configuration will be eth0. You need to change the interface to bond0 in order to reference the

bonded interface. See “Firewall Configuration” on page 86, or *The Advanced Administration Guide, Chapter 3*.

4. Select the **apply changes** button at the bottom of the application window to complete the procedure.

Syslog

The Syslog form allows you to configure one or more syslog servers to receive ACS-generated syslog messages. The ACS generates syslog messages related to users connecting to ports, login failures and other information that can be used for audit trailing purposes. You also use this form to delete syslog servers.

▼ To Configure Syslog

1. Select **Network > Syslog**

The system brings up the **Syslog** form.



Figure 4-24: Network Syslog Form

2. Complete the form as follows:

Table 4-15:

Field Name	Definition
Facility Number	Facility number to identify the location of the Syslog Server.
New Syslog Server	Name of the Syslog Server that you wish to add.
Syslog Servers	List of all Syslog Servers connected to ACS.

3. To add a new Syslog Server, type in the name of the server in the **New Syslog Server** field, and then select the **Add** button
4. - OR -
5. To delete a Syslog Server, from the **Syslog Servers** list box, select the server you wish to delete, and then select **Delete**.
6. Select **apply changes** to save your changes to Flash.

PCMCIA Management

The PCMCIA Management form allows you to configure the types of PCMCIA card that are installed in either one or both of the PCMCIA slots. ACS supports several PCMCIA cards including modem, ISDN, wireless and wired network cards, Compact Flash, and IDE drives for data buffer storage.

Note: For a list of the supported PCMCIA cards, refer to the AlterPath Advanced Console Server web site at http://www.cyclades.com/products/3/alterpath_acs, or go to www.cyclades.com > Products > IT Infrastructure Management > AlterPath ACS > Click here for a list of supported PCMCIA cards.

You can insert a card at any time and the corresponding driver should load automatically. Before removing a card, however, you must configure the PCMCIA form to eject the card and stop the system from using the card.

▼ **To Configure PCMCIA Cards**

1. Select **Network > PCMCIA Management**

The system brings up the PCMCIA Management form:

Configuring the ACS in Expert Mode

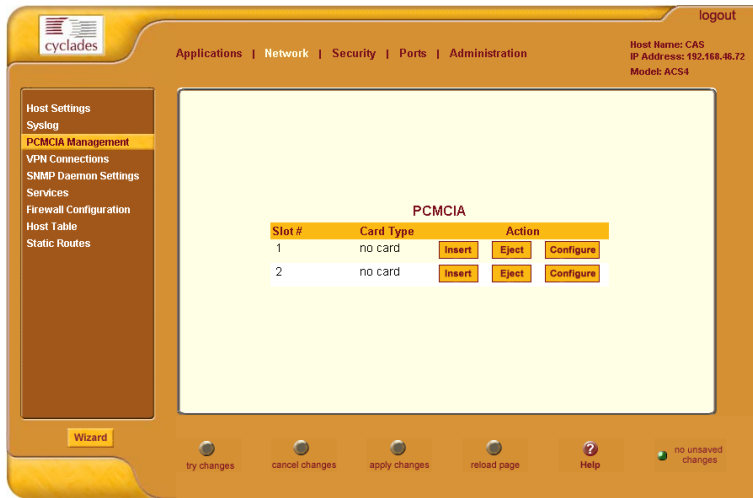
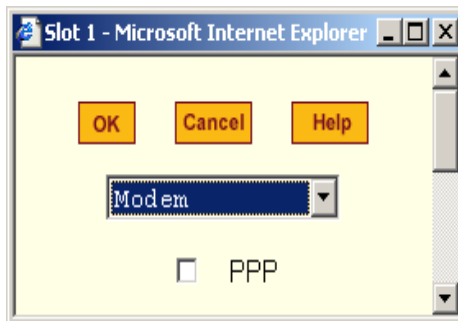


Figure 4-25:PCMCIA Management Form

2. Insert the card into the PCMCIA slot and then select the **Insert** button.
3. To configure the card, select the **Configure** button.
4. The system brings up the PCMCIA Configuration dialog box:



5. From the pull down menu, select the type of card that you are using.
6. Complete the rest of the dialog box. (See the succeeding **PCMCIA Configuration Dialog Boxes** section for information about each input field.)
7. Click on the **OK** button when done.
8. Click on **apply changes** to save your configuration.

PCMCIA Configuration Dialog Boxes

The ACS supports the following types of PCMCIA cards:

- Modem
- ISDN
- GSM
- Ethernet
- Compact Flash
- Wireless LAN

The dialog box for configuring the PCMCIA card will have varying sets of input fields depending on the type of PCMCIA card that you select from the drop down box:

Access Method: Modem

If the selected card type is *Modem* (default), the following fields are used:

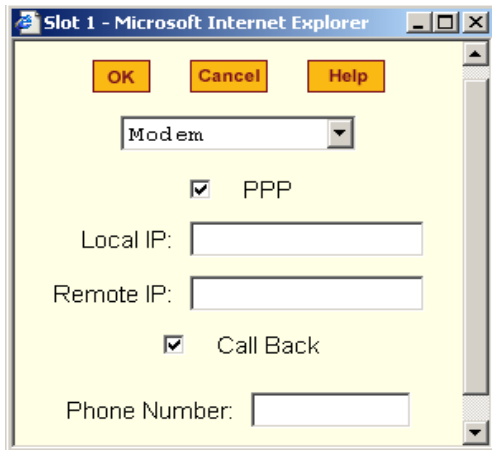


Table 4-16: Form Fields for a PCMCIA Modem Card

Field Name	Definition
[PCMCIA Card]	Pull-down box to select the type of PCMCIA card that you are using.
PPP	Check box to enable point-to-point protocol.

Table 4-16: Form Fields for a PCMCIA Modem Card

Field Name	Definition
Local IP	The local IP address of the PCMCIA card.
Remote IP	The remote IP address of the PCMCIA card.
Call Back	Check box to enable the callback security feature.
Phone Number	The phone number that the ACS uses to call back.

Access Method: ISDN

If the selected Access Method is *ISDN*, the following fields are used:

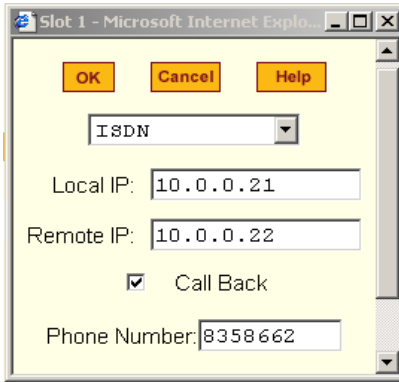


Table 4-17: Form Fields for an ISDN Card

Field Name	Definition
[PCMCIA Card]	Select ISDN from the pull-down box.
PPP	Check box to enable point-to-point protocol.
Local IP	The local IP address of the PCMCIA card.
Remote IP	The remote IP address of the PCMCIA card.
Call Back	Check box to enable the callback security feature.
Phone Number	The phone number that the ACS uses to call back.

Access Method: GSM

If the selected Access Method is *GSM*, the following fields are used:

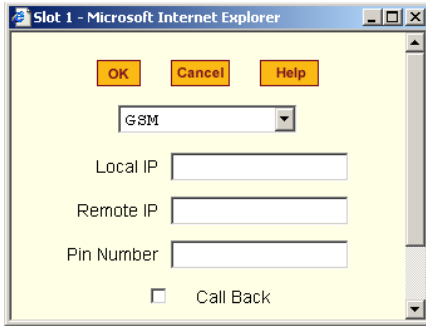


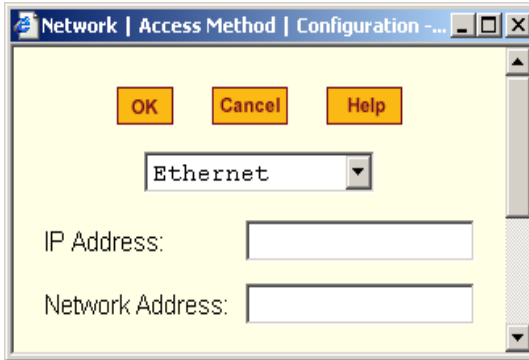
Table 4-18: Form Fields for a GSM Card

Field Name	Definition
[PCMCIA Card]	Select GSM from the pull-down box.
Local IP	The local IP address of the PCMCIA card.
Remote IP	The remote IP address of the PCMCIA card.
Pin Number	The personal identification number associated with the GSM.
Call Back	Check box to enable the callback security feature.

Access Method: Ethernet

If the selected Access Method is *Ethernet*, the following fields are used:

Configuring the ACS in Expert Mode



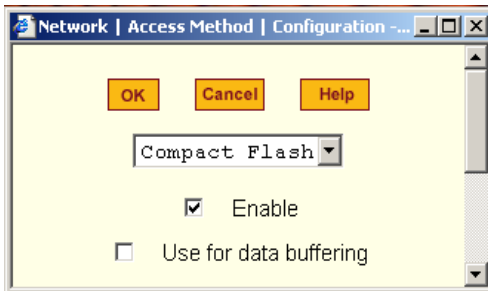
The screenshot shows a dialog box titled "Network | Access Method | Configuration". At the top are three buttons: "OK", "Cancel", and "Help". Below them is a pull-down menu currently set to "Ethernet". Underneath the menu are two text input fields: "IP Address:" and "Network Address:".

Table 4-19: Form Fields for an Ethernet LAN Card

Field Name	Definition
[PCMCIA Card]	Select Ethernet from the Pull-down box.
IP Address	The local IP address of the Ethernet.
Network Address	The network address of the Ethernet.

Access Method: Compact Flash

If the selected Access Method is *Compact Flash*, the following fields are used:



The screenshot shows a dialog box titled "Network | Access Method | Configuration". At the top are three buttons: "OK", "Cancel", and "Help". Below them is a pull-down menu currently set to "Compact Flash". Underneath the menu are two checkboxes: "Enable" (checked) and "Use for data buffering" (unchecked).

Table 4-20: Form Fields for a Compact Flash Card

Field Name	Definition
[PCMCIA Card]	Select Compact Flash from the Pull-down box.
Enable	Check box to enable the compact flash.

Table 4-20: Form Fields for a Compact Flash Card

Field Name	Definition
Use for Data Buffering	Check box to use the compact flash for data buffering.

Access Method : Wireless LAN

If the selected Access Method is *Wireless LAN*, the following fields are used:

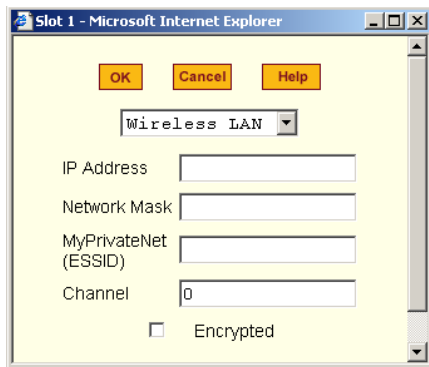


Table 4-21: Form Fields for a Wireless LAN Card

Field Name	Definition
[Unlabeled]	Pull-down box to select the type of PCMCIA card that you are using.
PPP	Check box to enable point-to-point protocol.
Local IP	The local IP address of the PCMCIA card.
Remote IP	The remote IP address of the PCMCIA card.
Call Back	Check box to enable the callback security feature.
Phone Number	The phone number that the ACS uses to call back.

What is VPN

*If you already understand how VPN works, skip this section and proceed to the next procedure, **Network > VPN Connections**.*

Configuring the ACS in Expert Mode

A VPN, or Virtual Private Network lets the Console Server and a whole network communicate securely when the only connection between them is over a third network which is not trustable. The method is to put a security gateway machine in the network and create a security tunnel between the Console Server and this gateway. The gateway machine and the Console Server 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 Console Server 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 Console Server), or between the Console Server and the Console Server administrator machine, which must, in this case, have a fixed IP address.

You can add this 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 leftnexthop (the router which Console Server sends packets to in order to get them delivered to right). Similarly, you may need to specify righnexthop (vice versa).

The Role of IPsec

IPsec is used mainly to construct a secure connection (tunnel) between two networks (ends) over a not-necessarily-secure third network. In ACS, the IPsec is used to connect the ACS securely to a host or to a whole network--configurations usually referred to as *host-to-network* and *host-to-host tunnel*. Practically, this is the same thing as a VPN, but here one or both sides have a degenerated subnet (*i.e.*, only one machine).

The IPsec protocol provides encryption and authentication services at the IP level of the network protocol stack. Working at this level, IPsec can protect any traffic carried over IP, unlike other encryption which generally protects only a particular higher-level protocol (PGP for mail, SSH for login, SSL for Web work and so on). The implementation of IPsec used by the ACS is FreeSWAN (www.freeswan.org).

You can use IPsec on any machine that does IP networking. Wherever required to protect traffic, you can install dedicated IPsec gateway machines. IPsec can also run on routers, firewall machines, various application servers, and end-user desktop or laptop machines.

Authentication Keys

To establish a connection, the Console Server and the other end must be able to authenticate each other. For FreeS/WAN, the default is public key authentication based on the RSA algorithm.

VPN Connections

The VPN configuration form allows you to configure one or more VPN connections to other systems or Cyclades ACS devices.

Select one of the existing VPN connections and click the edit button or click the add button to add a new one. This 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.

▼ To Configure VPN Connections

1. Select **Network > VPN Connections**

The system brings up the **VPN Connections** form:



Figure 4-26: VPN Connections Form

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 -

Configuring the ACS in Expert Mode

To add a VPN connection, select the **Add** button. The system brings up the **New/Modify VPN Connection** dialog box:

The screenshot shows a web browser window titled "New/Modify Connection - Microsoft Internet Explorer". The page has a yellow background and contains the following form fields:

- Buttons: OK, Cancel, Help
- Connection Name:
- Authentication Protocol:
- Authentication Method:
- Remote ("Right") section:
 - ID:
 - IP Address:
 - NextHop:
 - Subnet:
 - RSA Key:
- Local ("Left") section:
 - ID:
 - IP Address:
 - NextHop:
 - Subnet:
 - RSA Key:
- Boot Action:

If the selected **Authentication Method** is **RSA Public Keys**, the left dialog box is used. If the **Authentication Method** is **Shared Secret**, the right dialog box is used.

3. Edit or complete the appropriate fields from either dialog box as follows:

Table 4-22: Add/Modify VPN Connections Form Fields

Field Name	Definition
Connection Name	Name of the VPN connection.
Authentication Protocol	Authentication protocol used to establish a VPN connection.
Authentication Method	Authentication method used to establish a VPN connection.
Remote ("Right")	Set the following values:
ID	Identification name.
IP Address	Remote IP address.

Table 4-22: Add/Modify VPN Connections Form Fields

Field Name	Definition
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”)	Set the following values:
ID	Identification name.
IP Address	Local IP address.
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 RAS key.
Boot Action	Boot action with regards to generating an RSA key pair upon system boot.
Pre-Shared Secret	The pre-shared password between left and right users.

4. Select the **OK** button.
5. Select the **apply changes** button to save your configuration.

SNMP Daemon Settings

Short for Simple Network Management Protocol, SNMP is a set of protocols for managing complex networks. 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 ACS uses the Net-SNMP package (<http://www.net-snmp.org>). The Net-SNMP package contains various tools relating to the Simple Network

Configuring the ACS in Expert Mode

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. ACS supports SNMPv1, v2 and v3. The two versions require different configurations. SNMPv1/v2 requires community, source, object ID and the type of community (read-write, read-only). V3 requires user name.

Note: Check the SNMP configuration before gathering information about ACS by SNMP. There are different types of attacks an unauthorized user can implement to retrieve sensitive information contained in the MIB. By default, the SNMP configuration in ACS cannot permit the public community to read SNMP information.

▼ To Configure SNMP

1. Select **Networks > SNMP Daemon Settings**.

The system invokes the SNMP Daemon Settings form.

The screenshot shows the 'SNMP Daemon Settings' form in the ACS Web Manager. The interface includes a navigation menu on the left with options like 'Host Settings', 'System', 'PCMCIA Management', 'VPN Connections', 'SNMP Daemon Settings', 'Services', 'Firewall Configuration', 'Host Table', and 'Static Routes'. The main content area features a warning box: 'To activate the snmpd services, you should go to the Network Services section.' Below this are 'System Information Settings' with input fields for 'SysContact' and 'SysLocation', both containing the path '(configure /etc/snmp/snmpd.conf)'. There is an 'Access Control' section and an 'SNMPv1/SNMPv2 Configuration' table with columns for 'Community', 'Source', 'OID', and 'Permission'. At the bottom, there are buttons for 'Wizard', 'try changes', 'cancel changes', 'apply changes', 'reload page', 'Help', and 'no unsaved changes'.

Figure 4-27:SNMP Daemon Settings Form

2. Type in the following System Information, as necessary:

Table 4-23: System Information Settings

Field Name	Definition
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).

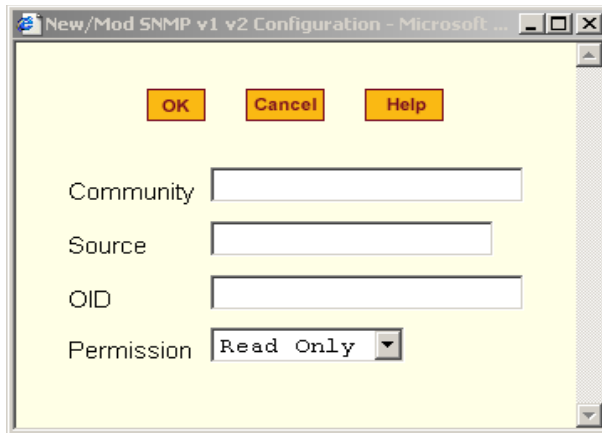
Note: If you are using SNMPv3, skip steps 2 and 3; proceed to step 4.

- To Add an SNMP agent using SNMPv1/SNMPv2 Configuration, select the **Add** button located at the bottom of the view table.

-OR-

- To Edit an SNMP agent, select the **Edit** button.

The system invokes the **New/Modify v1 v2 Configuration** dialog box.



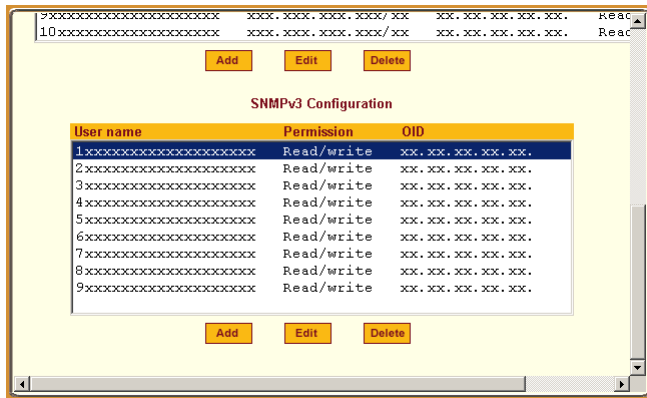
Configuring the ACS in Expert Mode

Complete the dialog box as follows:

Table 4-24: SNMP v1 v2 Configuration Dialog Box Fields

Field Name	Definition
Community	The password used to authenticate messages sent between the SNMP client and the router containing the SNMP server.
Source	The IP addresses or the range of source 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.• Admin - Read-write access.

3. If you are adding or editing an SNMP agent using SNMPv3, scroll down to the lower half of the SNMP Configuration form:



4. To Add an SNMP agent using SNMPv3 Configuration,

select the **Add** button located at the bottom of this view table.

- OR -

To edit an SNMP agent, select the **Edit** button.

The system invokes the **New/Modify SNMP v3 Configuration** dialog box:

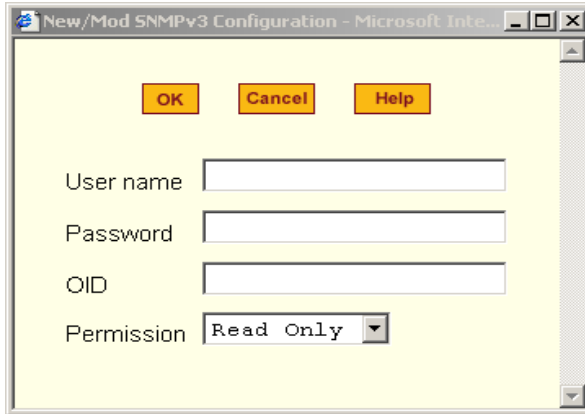


Figure 4-28:

5. Complete the form and select the **OK** button from the dialog box.
6. Verify your entry or modification from the respective tables of the SNMP Configuration form.
7. Select the **apply changes** button to complete the procedure.

Firewall Configuration

Firewall configuration, also known as *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 (*e.g.*, 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.

Structure of IP Filtering

The Firewall Configuration form is structured on two levels:

Configuring the ACS in Expert Mode

- The view table of the Firewall Configuration form which contains a list of chains.
- The chains which contain the rules that control filtering.

Chain

The filter table contains a number of built-in chains and can include any other chains that you add (user-defined chains) through the **Add Chain** dialog box. User-defined chains are called when a rule which is matched by the packet points to the chain.

The built-in chains are called according to the type of packet, and are classified as follows:

- INPUT - For packets coming into the ACS box itself.
- FORWARD - For packets being routed through the ACS box.
- OUTPUT - For locally-generated packets.

Rule

Each chain has a sequence of rules that address the following:

- How the packet should appear in order to match the rule.
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.
- What to do when the packet matches the rule.
The packet can be accepted, blocked, logged or jumped to a user-defined chain.

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.

▼ **To Configure The Firewall**

- Select **Network > Firewall Configuration**

The system brings up the Firewall Configuration form.

As explained in the last section, this form lists the chains that make up the rules for IP filtering.

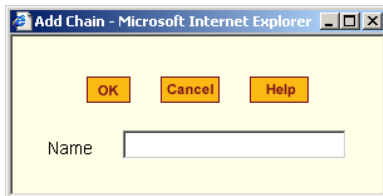


Figure 4-29: Network Firewall Configuration Form

Adding a Chain

1. From the Firewall Configuration form, click on the **Add** button.

The system brings up the **Add Chain** dialog box:



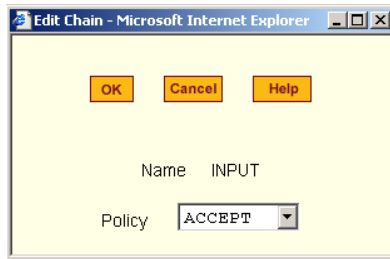
2. Type in the chain name in the **Name** Field, and then select **OK**. (Spaces are not allowed in the chain name.)
3. After entering a new chain name, click on the **Edit Rules** button to access the next dialog window to enter the rules for that chain.
4. Select **OK** to commit your changes.
5. To add rules to your new chain, proceed to the *Adding a Rule* section.

Editing a Chain

1. To edit a chain, select from the view table the chain you wish to edit and then select the **Edit** button.

Configuring the ACS in Expert Mode

The system brings up the **Edit Chain** dialog box:



2. Modify the **Policy** field, as necessary, and then select the **OK** button.
3. If you need to edit any rules for this chain, proceed to the *Editing a Rule* section.

Deleting a Chain

Only user-defined chains can be deleted. The system will not allow you to delete a built-in chain.

1. From the Firewall Configuration form, select the chain you wish to delete from the list, and then select the **Delete** button.

Editing a Rule

The rules define how the filtering should work. To edit a rule, choose from the **Edit Rule** dialog box the target policy (Accept/Reject/Log/Return/Drop) and the packets you want to filter (source/destination IP, Ethernet interface and protocol type, if it applies to fragments). Any of the items (*i.e.*, source/destination IP, input/output interface) can be inverted by checking the **Inverted** check box. To invert means, rules will apply to everything except for the (adjacent) item just defined.

1. From the Firewall Configuration form, select the chain containing the rule(s) that you wish to edit, and then click on the **Edit Rule** button.

The system brings up the **Edit Rules for Chain** form:

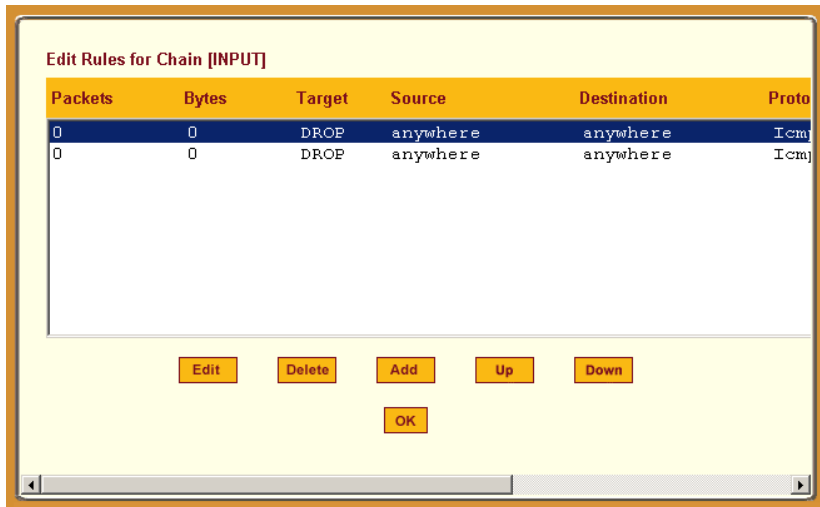


Figure 4-30: Edit Rule Form

2. From the **Edit Rules for Chain** form, select the rule you wish to edit, and then click on the **Edit** button. Use the **Up** and **Down** buttons to navigate through the list, as necessary.
3. The system brings up the **Edit Rule** dialog box:

Configuring the ACS in Expert Mode

OK Cancel Help

Target
ACCEPT

Source IP 0.0.0.0 Mask 0 Inverted
Destination IP 0.0.0.0 Mask 0 Inverted
Protocol ICMP Inverted
Input Interface Inverted
Output Interface Inverted
Fragments All packets

ICMP Options Section
ICMP Type
timestamp-request Inverted

4. Complete the necessary fields as follows:

Table 4-25: Edit Rule Dialog Box Fields

Field Name	Definition
Target	Indicates the action to be performed to the IP packet when it matches the rule. The kernel can be configured to 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.

Table 4-25: Edit Rule Dialog Box Fields

Field Name	Definition
Inverted	Select box to invert the target action (<i>i.e.</i> , 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 box to invert the target action (<i>i.e.</i> , 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 text input field; otherwise, select one of the other options.
Inverted	Select box to invert the target action (<i>i.e.</i> , the action assigned to the target will be performed to all protocols except to the one just defined).
Interface	The interface where the IP packet should pass.
Inverted	Select box to invert the target action (<i>i.e.</i> , 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 firewall (<i>i.e.</i> , IP Tables) can check for: <ul style="list-style-type: none"> - All Packets. - 2nd, 3rd... fragmented packets. - Non-fragmented and 1st fragmented packets.

Table 4-25: Edit Rule Dialog Box Fields

Field Name	Definition
ICMP Options Section	Select from the scrollable list the error message to be associated with the rule. ICMP is the internet protocol sent in response to errors in TCP/IP messages (i.e., IP datagrams or packets), between a host and a gateway. The messages are processed by the IP software and are transparent to the application user.

Additional Fields

If you selected Log as the Target, the following additional fields appear:

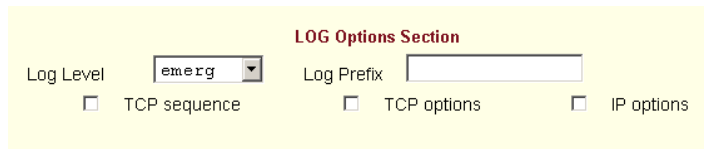


Table 4-26: Edit Rule Log Options

Field Name	Definition
Log Level	The log level classification to be used based on the type of error message (e.g., alert, warning, info, debug, etc.).
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 as the target, the **Reject Options** field appears:



REJECT Options Section

Reject with

5. From the scrollable list, select the ICMP message to be associated with the Reject target.
6. Click on the **OK** button when done.
7. Click on the **apply changes** located at the bottom of the ACS configuration window to save your configuration.

Adding a Rule

The forms and dialog boxes for adding a rule is similar to the ones used for editing a rule. Refer to the *Editing a Rule* procedure section for a definition of the user input fields.

1. From the **Firewall Configuration** form, select the chain to which you wish to add a rule (or if you are adding a new chain, select the **Add** button and follow the procedure for *Adding a Chain*.)
2. Click on the **Edit Rule** button.
3. The system brings up the **Edit Rule for Chain** dialog box.
4. From the **Edit Rule for Chain** dialog box, click on the Add button.
5. The system brings up the **Add Rule** dialog box.
6. Complete the Add Rule dialog box. (Refer to the *Editing a Rule* section for a definition of the input fields, as needed.)
7. Click on the **apply changes** button located at the bottom of the ACS configuration window to complete the procedure.

About the Reject Options Section

When **Reject** is selected as the target, the **Reject Options Section** appears with the following fields:

Table 4-27: Reject Options Section Fields

Field Name	Definition
Reject with	("Reject with" means that the filter will drop the input packet and send back a reply packet according to any of the reject types listed below.)
Choices are:	
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.

Note: *The packets are matched (using tcp flags and appropriate reject type) with the REJECT target.*

Host Table

The Host Table 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 The Host Table**

1. Select **Network > Host Table**.

The system invokes the Host Tables form



Figure 4-31: Host Table Form

2. To edit host, select the host IP address from the Host Table and then click on the **Edit** button. (If the list is long, use the **Up** and **Down** buttons to go through each item in the list.)

- OR -

3. To add a host, click the **Add** button.
4. The system brings up the **New/Modify Host** dialog box:

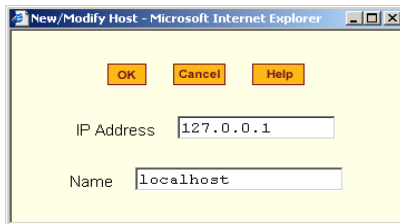


Figure 4-32:

5. Type in the new or modified host address in the **IP Address** field, and the host name in the **Name** field, and then select the **OK** button.
6. To delete a host, select the host you wish to delete from the Host Table form, and then select the **Delete** button from the form.
7. Select the **apply changes** button 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.

You can add or edit a hard-coded static route by clicking on the corresponding buttons. They'll bring you to a dialog box to enter the route to be added. To delete a static route, highlight the route and then select the **Delete** button.

▼ To Configure Static Rules

1. Select **Network > Static Routes**.

The system brings up the Static Routes table form:



Figure 4-33: Static Routes Form

Note: Refer to the field definitions in Step 3 for the meaning of each field in the table.

2. To edit a static route, select a route from the Static Routes form, and then select the **Edit** button.

- OR -

3. To add a static route, select the **Add** button from the form.

4. The system invokes the **New/Modify Route** dialog box:

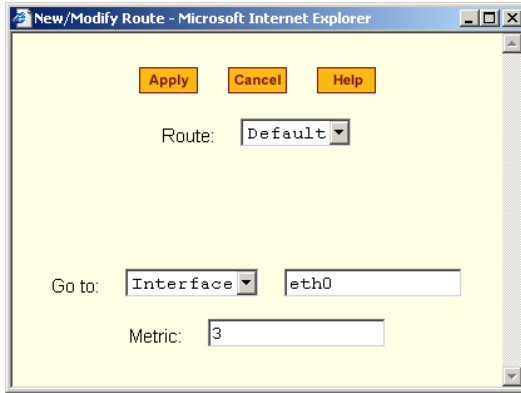


Figure 4-34:

5. Complete the fields as follows:

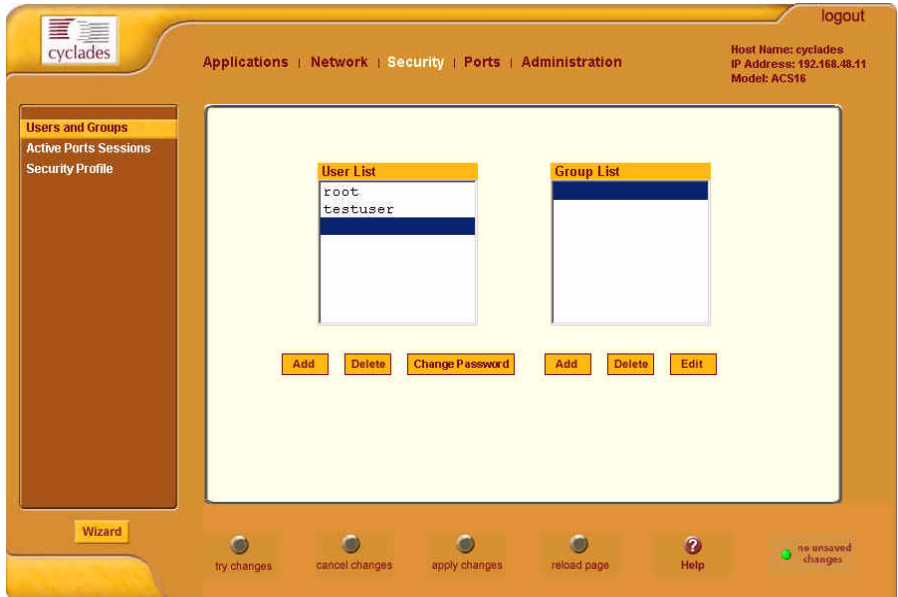
Table 4-28: New/Modify Route Dialog Box Fields

Field Name	Definition
Route	Select Default , Network , or Host .
Network IP	<i>This field appears only if Network is selected.</i> The address of the destination network.
Network Mask	<i>Only if Network is selected.</i> The mask of the destination network.
Host IP	<i>Only if Host is selected.</i> The IP address of the destination host.
Go to (Adjacent field)	Select Gateway or Interface . The address of the gateway or interface.
Metric	The number of hops.

6. Select **Apply** when done.

Security

The Security configuration of the ACS, as shown by the left menu panel includes the following configuration forms.



- Users and Groups
- Active Ports Sessions
- Security Profile

Users and Groups

Users and Groups configuration allows you to set up users to have access to the ACS web application, assign them to specific groups that share common access rights, as well as assign or re-assign passwords. Moreover, you can create new groups to add to the group list.

The access limits provide privileges based on the functionality of the Web page.

The two groups to which you can assign a user are:

- **Admin** - Read/Write Access
- **Regular User** - Limited R/W Access

Although **root** is also a user, there is only one root user (username *root*, default password *tslinux*).

Note: If a step does not apply (*e.g.*, edit, delete), skip to the next step.

▼ **To Add Users and Groups to the Access List**

1. From the top menu bar, select **Security**; from the left menu panel, select **Users and Groups**.

The system brings up the Users and Groups form:

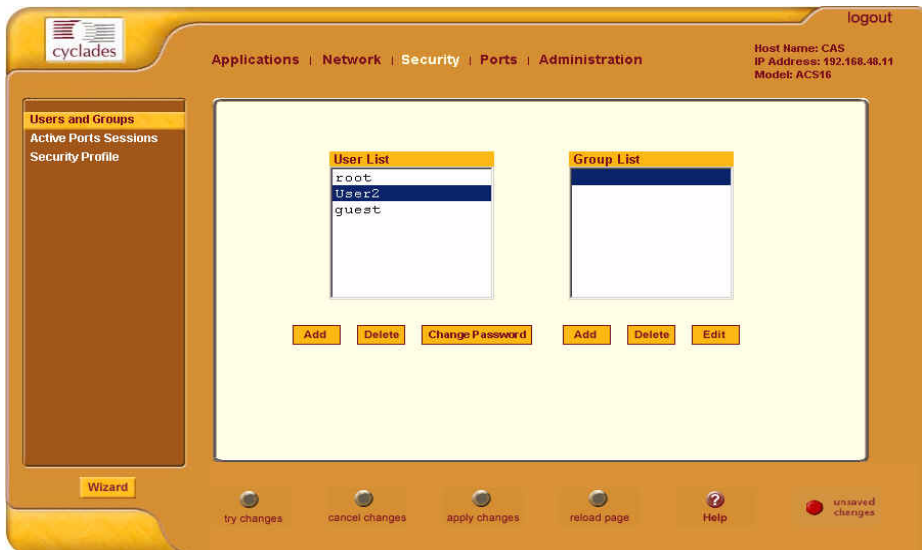
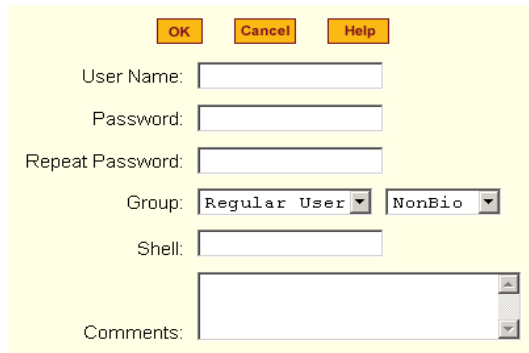


Figure 4-35: Users and Groups Form

2. To add a user to the **User list** OR to add a group to the **Group list**, select the **Add** button at the bottom of the corresponding list box.
3. The system brings up the **Add Users and Groups** dialog box:

Configuring the ACS in Expert Mode



4. Complete the dialog box shown above, and then select **OK**.

Note: All users must be assigned to a group.

5. To edit a user or a group, from the Users and Groups form, select the user or the group you wish to edit from the appropriate listbox, and then select the **Edit** button located at the bottom of the corresponding listbox.
6. Repeat step 3.

▼ **To Delete a User from a Group**

1. To delete a user, select the user name you wish to delete from the User List of the Users and Groups form, and then select the **Delete** button at the bottom of the list box.
- OR -
2. To delete a group, select the group name from the Group listbox of the Users and Groups form, and then select the **Delete** button.

▼ **To Change the User Password**

1. To change a user's password, select the user whose password you wish to change from the User List, and then select the **Change Password** button.
The system brings up the Change Password dialog box.
2. Complete the Change Password dialog box and then select **OK**.
3. From the bottom of the main ACS window, select **apply changes** to save your configuration to Flash.

Active Ports Sessions

The Active Ports Sessions window is designed to provide you a quick status, and usage information (for example, user, tty, Login time, JCPU, *etc.*) pertaining to all active ports sessions.

Open sessions are displayed with their identifications and statistical data for login, session and CPU usage for the specific client. JCPU relates all processes attached to that port including running background processes. PCPU relates the current processing time.

- Select **Security > Active Ports Sessions**.

The system invokes the Active Ports Sessions form.

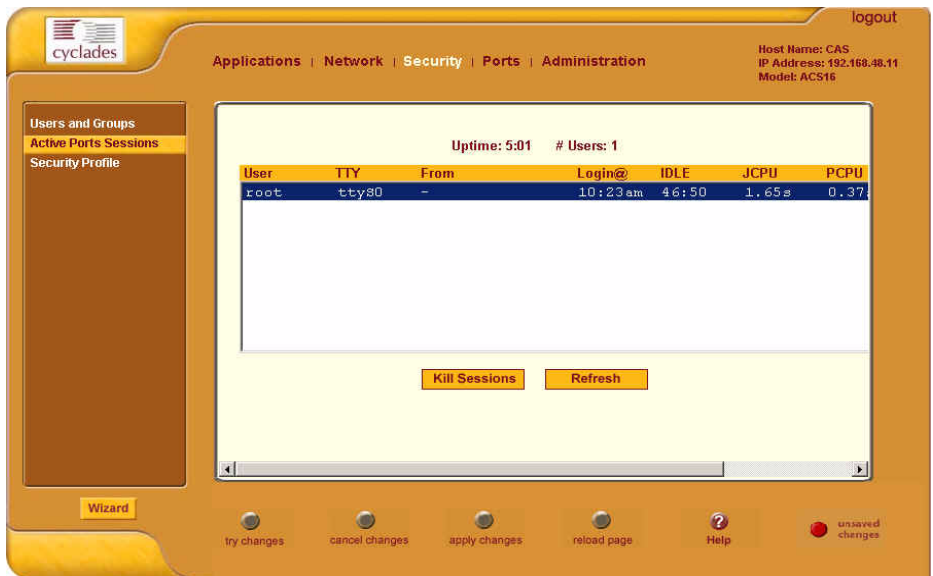


Figure 4-36: Active Port Sessions Form

Table 4-29: Active Port Session Fields

Field Name	Definition
User	The user who initiated the port session.
TTY	The name of the serial port.

Table 4-29: Active Port Session Fields

Field Name	Definition
From	The network machine to which the port is connected.
Login	The time of the last login.
Idle	The time when the port 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.

Security Profile

The first step in configuring AlterPath ACS is to define a Security Profile. A Security Profile consists of a set of parameters that can be set to control access to the ACS. There are three pre-defined security profiles, **Secured**, **Moderate**, **Open**, and an option to configure a **Custom** profile. A fifth option, **Default** will set the parameters to the same as **Moderate**. See "Configuring the Security Profile in Wizard Mode" on page 38 for detailed definition of each profile.



Figure 4-37: Security Profile Form

1. From the main entry panel select a pre-defined Security Profile and click on **apply changes**.

OR

2. Click on **Custom** to define services individually.

The system brings up the following Custom Profile window.

Configuring the ACS in Expert Mode

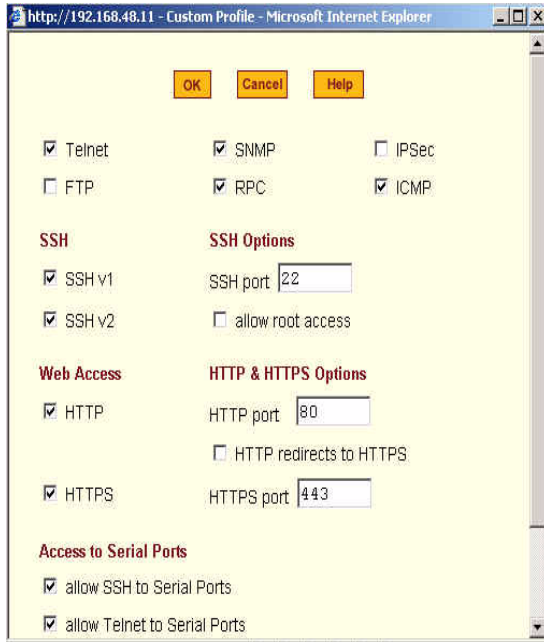


Figure 4-38: Custom Security Profile Dialog Box

3. Enable or disable services, configure ports, and configure access to the Serial Ports.
4. Click on **apply changes**.

Ports

The Ports section of the ACS configuration in Expert Mode provides three menu choices:

- **Physical Ports:** Allows you to view and modify the physical port settings.
- **Virtual Ports:** Allows you to view and modify the slave port settings.
- **Ports Status:** Provides a read-only view on status of each physical port, its signal status, and the current active user.

Physical Ports

The **Physical Ports** form is used to select the ports you wish to configure (*i.e.*, all ports or individually selected ports). Once you have selected the port(s) to configure, you will have access to five tabbed forms to configure any of the following:

Table 4-30: Physical Ports Form Fields

Tab Name	Use this form to:
General	Define general port settings; Connect to an IPDU port and select the connection type (SSH, Telnet or both).
Access	Designate users and groups to authenticate, and assign authentication type or server.
Data Buffering	Define data buffering mode, size, syslog server, etc.
Multi User	Enable concurrent usage and sniff mode.
Power Management	Enable Power Management for the selected port(s); assign users and groups to enable them to set the IPDU settings for these port(s).
Other (port settings)	Configure other port settings such as break interval, login banner, PPP options, etc.

▼ To Modify Port Access

1. From the top menu, select **Ports**; from the left menu, select **Physical Ports**.

Note: By default, all Serial Ports are disabled. The Administrator can activate and assign specific users to individual physical ports.

The system invokes the Physical Ports Modification form:

The screenshot shows the Physical Ports Modification form in the Cyclades web interface. The form has a sidebar on the left with 'Physical Ports', 'Virtual Ports', and 'Ports Status' options. The main content area contains a table of physical ports and four buttons: 'Modify Selected Ports', 'Modify All Ports', 'Enable Selected Ports', and 'Disable Selected Ports'. The table has the following data:

Port	Disable	Alias	Connection Protocol	Serial Config
1			Console (Telnet)	9600 8N1
2		pm10	IPDU	9600 8N1
3			Console (Telnet)	9600 8N1
4			Console (Telnet)	9600 8N1

The bottom navigation bar includes a 'Wizard' button and five circular buttons: 'try changes', 'cancel changes', 'apply changes', 'reload page', and 'Help'. A 'no unsaved changes' indicator is visible in the bottom right corner.

Figure 4-39:Physical Ports Form

This form allows you to:

- Modify all or only selected ports.
 - Enable or disable selected ports.
2. To modify selected ports, select the port you wish to modify from the Physical Ports Modification form, and then click on the **Modify Selected Ports** button.
- OR -
3. To modify all ports, click on the **Modify All Ports** button.
 4. Proceed to the next section, **Configuring Ports** and select the tabbed form you wish to configure.

▼ **To Associate an Alias to a Port**

A name (alias) can be associated to a port when it's individually selected for modification. To associate an alias to a port perform the following steps.

1. While in Expert Mode, go to: **Ports > Physical Ports**.
2. From the **Physical Ports** (Selection) form, select the port to configure and then click on the **Modify Selected Ports** button.
3. The system displays the Modify Selected Port form:

The screenshot shows a web-based configuration interface for a port. At the top, there are several tabs: 'General', 'Access', 'Data Buffering', 'Multi User', 'Power Management', and 'Other'. The 'General' tab is selected. Below the tabs, there are several configuration fields: 'Connection Protocol' is a dropdown menu set to 'Console (Telnet)'; 'Alias' is a text input field containing 'tst1'; 'Baud Rate (Kbps)' is a dropdown menu set to '9600'; 'Flow Control' is a dropdown menu set to 'None'; 'Data' is a numeric input field set to '8'; 'Parity' is a dropdown menu set to 'None'; and 'Stop Bits' is a numeric input field set to '1'. At the bottom of the form, there is a 'Done' button and a status indicator that says 'Selected ports #: 2'.

Figure 4-40: Port Modification Form

Note: The **Alias** field cannot be set if you select the **Modify All Ports** button.

4. From the **Alias** field, enter the port alias using one or more strings separated by spaces.
5. Click on the **apply changes** button to save your configuration.

General Port Configuration

The **General** form is used to define the port profile for the selected port(s).

1. From the top menu, select **Ports**; from the left menu, select **Physical Ports**.

Configuring the ACS in Expert Mode

The system invokes the **General** tabbed form:

The screenshot shows the 'Serial Ports General Modification Form' in the 'cyclades' Web Manager. The form is titled 'General' and includes the following fields and options:

- Connection Protocol: Console (SSH)
- Alias: [Empty text box]
- Baud Rate (Kbps): 9600
- Flow Control: None
- Data: 8
- Parity: None
- Stop Bits: 1
- DCD State: Disregard

The interface also shows a sidebar with 'Physical Ports', 'Virtual Ports', and 'Ports Status', and a bottom navigation bar with buttons for 'try changes', 'cancel changes', 'apply changes', 'reload page', 'Help', and 'no unsaved changes'.

Figure 4-41: Serial Ports General Modification Form

2. Complete the form as follows:

Table 4-31: Serial Port Modification Form Fields

Field Name	Definition
Connection Protocol	The connection protocol to be used by the selected port. Choices are: Console (Telnet), Console (SSH), Console (Raw), Telnet, SSHv1, SSHv2, Local Terminal, Raw Socket, PPP-No Auth, PPP, SLIP, CSLIP, and Power Management.
Alias	Port alias, if applicable.
Baud Rate (Kbps)	9600 Kbps is the default rate for most servers.
Flow Control	Choices: None, Hardware, or Software.
Data	The number of data bits.
Parity	Port parity -- none, even, or odd.
Stop Bits	The end of the data type

Table 4-31: Serial Port Modification Form Fields

Field Name	Definition
DCD State	Data Carrier Detect Signal, Regard or Disregard

3. Click on the **apply changes** button at the bottom of the ACS configuration window to save your port settings.

Access - Power Management

There are three ways in which the General form allows you to access Power Management:

- SSH
- Telnet
- SSH and Telnet

1. Go to **Ports > Physical Ports > General**.
2. From the **Connection Protocol** pull down menu of the General tabbed form, select **Power Management**.
3. The system invokes new fields for selecting the connection type.
4. From the invoked dropdown entry field (**Allow Access by**), select the desired connection type.

Configuring the ACS in Expert Mode



Figure 4-42: Serial Ports Access Modification Form

5. The system activates the **Access** and **Other** tabs.
6. If you selected SSH and/or Telnet, select the **Access** tab.
7. From the **Access** tabbed form, configure the authentication method for SSH and/or Telnet, as selected from the previous form.
8. If Biometric authentication is required, select and complete the **Other** tabbed form.
9. Click on **apply changes** to save your configuration to Flash.

Access - User and Group Setup

The Access form of the Ports menu is used to assign users and groups to an authentication services. You also select the authentication service from this form.

A summary of authentication services that you can configure from this form is as follows:

Table 4-32: Serial Ports Access Modification Form Fields

Authentication Type	Definition
None	No authentication.
Local	Authentication is performed locally (<i>i.e.</i> , using the /etc/passwd file).
Remote	This is for a terminal profile only. The unit takes in a username but does not use it for authentication. Instead it passes it to the remote server where it is then used for authentication.
Radius	Authentication is performed using a Radius authentication server.
TacacsPlus	Authentication is performed using a TacacsPlus authentication server.
Ldap	Authentication is performed against an ldap database using an ldap server.
Kerberos	Authentication is performed using a Kerberos server.
Local/Radius	Authentication is performed locally first, switching to Radius if unsuccessful.
Radius/Local	The opposite of the previous option.
Local/TacacsPlus	Authentication is performed locally first, switching to TacacsPlus if unsuccessful.
TacacsPlus/Local	The opposite of the previous option.
RadiusDownLocal	Local authentication is tried only when the Radius server is down.
TacacsPlusDownLocal	Local authentication is tried only when the TacacsPlus server is down.
kerberosDownLocal	Local authentication is tried only when the kerberos server is down.

Table 4-32: Serial Ports Access Modification Form Fields

Authentication Type	Definition
ldapDownLocal	Local authentication is tried only when the ldap server is down.
NIS	All authentication types but NIS follow the format all.authtype <Authentication>DownLocal or <Authentication> (e.g. all.authtype radius or radiusDownLocal or ldap or ldapDownLocal, etc). NIS requires all.authtype to be set as local, regardless if it will be "nis" or its "Downlocal" equivalent.

▼ **To configure user/group authentication**

1. From the top menu, select **Ports**; from the left menu, select **Physical Ports**; from the form tab menu, select **Access**.

The system brings up the **Access** form:

The screenshot shows a web-based configuration interface. At the top, there are several tabs: 'General', 'Access', 'Data Buffering', 'Multi User', 'Power Management', and 'Other'. The 'Access' tab is currently selected. Below the tabs, there are two main input fields: 'Authorized Users/Groups' which is a text box, and 'Type' which is a dropdown menu currently showing 'None'. At the bottom of the form area, there is a status bar that reads 'Selected ports #: 1' and a 'Done' button.

2. Enter the user or the group name.
3. From the **Type** drop down list, select the authentication type.

Entry Fields Based on Authentication Type

The user entry fields that are available from the Access form depend on the authentication type that you select from the **Type** field.

Authentication: Radius

- Authorized Users/Groups
- First Authentication Server
- (Hostname)
- Second Authentication Server
- (Hostname)
- First Accounting Server
- (Hostname)
- Second Accounting Server
- (Hostname)
- Secret
- Timeout
- Retries

Authentication: LDAP or LdapDownLocal

When you select LDAP, authentication is performed against an LDAP database using an LDAP server. Selecting LdapDownLocal means that authentication is tried on

- LDAP Server
- LDAP Base Domain Name
- Secure LDAP

Authentication Type: NIS, LocalNIS or NISLocal (All ACS only)

- Authorized Users/Groups
- NIS Domain Name
- NIS Server IP

Authentication Type: Kerberos, KerberosDownLocal

- **Kerberos** The server performing the authentication.

Configuring the ACS in Expert Mode

- **KerberosDownLocal** Local authentication is tried only when the kerberos server is down
 - Authorized Users/Groups
 - Kerberos Server (Realm)
 - Kerberos Realm
 - Domain Name

Data Buffering

1. From the top menu, select **Ports**; from the left menu, select **Physical Ports**; from the Physical Ports form, select the ports to modify; from the resulting form, select the **Data Buffering** tab.

The system brings up the Data Buffering form. The form below shows both checkboxes (**Enable Data Buffering** and **Buffer to Syslog**) selected to reveal all the form fields:

The screenshot shows the 'Data Buffering' configuration form. The 'Data Buffering' tab is active, and both 'Enable Data Buffering' and 'Buffer to Syslog' are checked. The 'Destination' is set to 'Local', 'Mode' is 'Circular', and 'File Size (Bytes)' is '0'. The 'Record the timestamp in the data buffering file' checkbox is unchecked. The 'Show Menu' is set to 'Show all options'. The 'Syslog Server' field is empty, and the 'Facility Number' is set to 'Local0'. The 'Syslog Buffer Size' is '0'. The 'Buffer SysLog at all times' radio button is selected. The status bar at the bottom indicates 'Selected ports #: 1' and a 'Done' button.

Figure 4-43:Data Buffering Form

2. Complete the necessary fields as follows:

Table 4-33: Data Buffering Form Fields

Field Name	Definition
Destination	Select whether the destination of the data buffer is Local or Remote.

Table 4-33: Data Buffering Form Fields

Field Name	Definition
Mode	Select whether the Buffering Mode is Linear (sequential) or Circular (non-sequential).
Full Size (Bytes)	The maximum limit of the data buffer.
Record the timestamp...	Commands the system to include a timestamp in the data buffering file.
Show Menu	Indicates the menu type for viewing the buffer. Select from: Show all options, No, Show data buffering file only, and Show without the erase options.
Syslog Server	The IP address of the Syslog Server.
Facility Number	Facility or location ID of the Syslog Server.
Syslog Buffer Size	Maximum size of the buffer.

By selecting the appropriate radio button, you can configure ACS to:

- **Buffer Syslog at all times.**
- **Buffer only when nobody is connected to the port.**

Note: To configure data buffering to send alarm notifications, use the Notifications form (Expert Mode: **Administration > Notifications**).

3. When done, select the **apply changes** button located at the bottom of the ACS configuration window.

Multi-User

The Multi User form enables you to open more than one common and sniff session (multiple sessions) from the same port.

If configured as **No** (*i.e.*, do not allow multiple sessions), only two users can connect to the same port simultaneously. If configured as **Yes**, more than two simultaneous users can connect to the same serial port.

Configuring the ACS in Expert Mode

A Sniffer menu is presented to the user and they can choose to:

- Open a sniff session
- Open a read and/or write session
- Cancel a connection
- Send a message to other users connected to the same serial port.

If it is configured as RW, only read and/or write sessions will be opened, and the sniffer menu won't be presented.

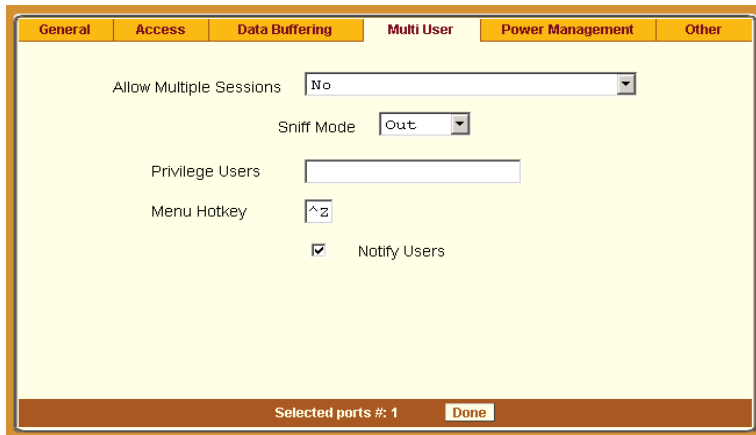
If configured as "sniff_session" only, a sniff session will be opened, and the sniffer menu won't be presented. Default value: no.

▼ **To configure ACS to allow multiple sessions**

1. Select **Ports** from the top menu bar; select **Physical Ports** from the left menu panel.

The system brings up the Physical Ports list.

2. From the Physical Ports list, select the Port(s) you wish to modify (to enable multiple sessions).
3. Select the **Multi User** tab from the resulting form.
4. The system invokes the Multi User form:



The screenshot shows a configuration window with a yellow background and a brown border. At the top, there are six tabs: General, Access, Data Buffering, Multi User, Power Management, and Other. The 'Multi User' tab is selected. Below the tabs, there are several configuration options:

- 'Allow Multiple Sessions' is a dropdown menu currently set to 'No'.
- 'Sniff Mode' is a dropdown menu currently set to 'Out'.
- 'Privilege Users' is an empty text input field.
- 'Menu Hotkey' is a text input field containing '^Z'.
- 'Notify Users' is a checkbox that is checked.

At the bottom of the window, there is a status bar that says 'Selected ports #: 1' and a 'Done' button.

Figure 4-44:Multi User Form

5. Complete the form as follows:

Table 4-34: Multi User Form Fields

Field Name	Definition
Allow Multiple Sessions	Select from: No, Yes (show menu), Read/Write (do not show menu), ReadOnly (do not show menu).
Sniff Mode	Select from: Out, In, In/Out, and No.
Menu Hotkey	The hotkey for accessing the menu.
Notify Users	Check box to notify users of session access.

When multiple sessions are allowed for one port, ACS will accept only one common session and one sniffer session. In this setting, the behavior of the ACS is as follows:

- The first user to connect to the port opens a common session.
- From the second connection on, only **Admin** users are allowed to connect to that port.
- The ACS will send a hotkey menu to the administrator(s).

Power Management

The Power Management form of the Ports menu is used to enable power management for the current port, add and delete power management ports, and assign user and group access to these ports.

▼ *To Configure Ports for Power Management*

1. Select **Ports** from the top menu; select **Physical Ports** from the left menu; select **Power Management** from the row of tabs.

The system brings up the **Power Management** form:

Configuring the ACS in Expert Mode

The screenshot shows the 'Power Management' tab of the ACS configuration interface. It includes a checked checkbox for enabling power management, a table for defining power management ports and outlet numbers, an 'Add' button, a 'Delete' button, a 'Power Management Key' input field, and radio buttons for 'Allow All Users' and 'Allow Users/Groups'. An 'Allowed Users/Groups' list box is also visible, along with a status bar showing 'Selected ports #: all' and a 'Done' button.

Figure 4-45: Serial Ports Power Management Form

2. Complete the form as follows:

Table 4-35: Serial Ports Power Management Form Fields

Field Name	Definition
Enable Power Management on this Port	Check mark to enable Power Management on the the selected port(s).
Power Management Port	View listbox for the PM ports and the assigned outlet numbers.
Power Management Key	The key sequence which the allowed user(s) can use to perform power management.
Allow All Users	Radio button to allow all users to perform power management on this port.
Allow Users/Groups	Radio button to allow only selected users or groups to perform power management on this port.
Allowed Users/Groups	View List Box of Allowed Users or Groups. Use the Delete or Add button to maintain this listbox.

3. Select the **apply changes** button at the bottom of the ACS configuration window to save your configuration.

Other Setting

The **Other** form is used to define less commonly used port settings such as the Port IP Alias, STTY options, TCP keepalive intervals, enabling Windows EMS, and the like.

▼ To Configure Other Port Settings

1. Select **Ports** from the top menu; select **Physical Ports** from the left menu; select **Other** from the row of tabs.

The system brings up the last tabbed form for **Physical Ports**:

The screenshot shows a configuration window with the following fields and values:

- Port IP Alias: []
- TCP Port: 7001
- Windows EMS:
- TCP Keep-alive Interval: 1000
- Idle Timeout: 0
- STTY Options: []
- Break Interval: 500
- Login Banner: " Welcome to Console Server Management Server %h port %p "

At the bottom, it says "Selected ports #: all" and a "Done" button.

Figure 4-46: Physical Ports Form (Other Tab)

2. From the above form, complete the following fields, as necessary:

Table 4-36: Physical Ports From Fields (Other Tab)

Field Name	Definition
Port IP Alias	The IP alias of the selected port.
TCP Port	The TCP Port number.
Port Name	As indicated.

Table 4-36: Physical Ports From Fields (Other Tab)

Field Name	Definition
Windows EMS	Checkbox to enable Windows EMS (Expanded Memory).
TCP Keep-alive Interval	Specifies the time interval between the periodic polling by the system to check client processes and connectivity.
Idle Timeout	The maximum time (in seconds) that a session can be idle before the user is logged off.
STTY Options	Set terminal options.
Break Interval	Break interval in milliseconds.
Login Banner	Text entry field box. Enter the text you wish to appear as a login banner upon logging onto the terminal.
Host to Connect	Address of the host connected to the port.
Terminal Type	As indicated.
Modem Initialization	Text entry field box.
PPP Options	Options when using this protocol.

Virtual Ports

You can use one ACS as a Master to control other ACS units (slaves). The ports on the slave unit acts as an extension of the master unit. The Virtual Ports form is used to add, edit or delete these virtual ports or slaves.

1. From the top menu, select **Ports**; from the left menu, select **Virtual Ports**.

The system brings up the **Virtual Ports (Slave)** form

▼ **To Add or Edit a Slave**

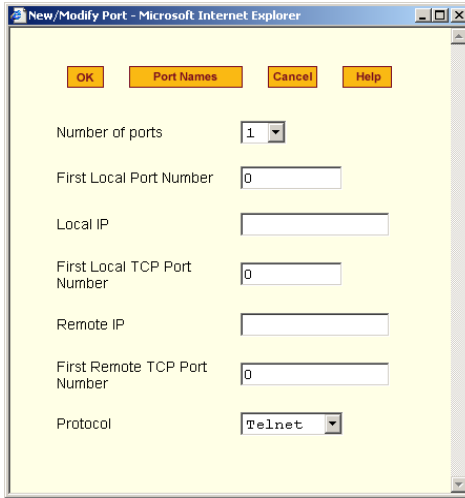


Figure 4-47: Virtual Ports Form

1. To add a new slave, select the **Add** button
- OR -
2. To edit a slave, select the slave you wish to edit from the Slave list.

The system brings up the **New/Modify Port** dialog box:

Configuring the ACS in Expert Mode



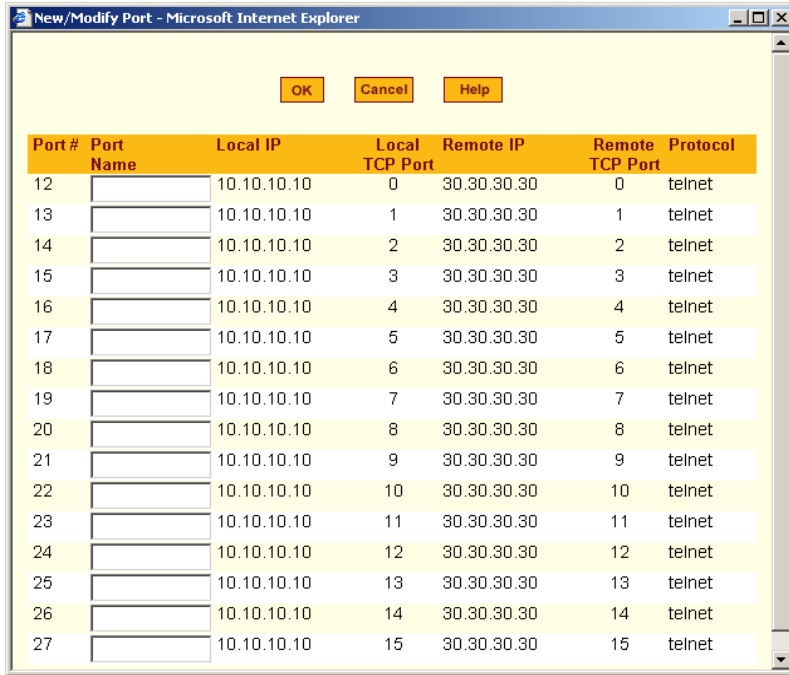
3. Complete the dialog box.

Table 4-37: New/Modify Port Dialog Box Fields

Field Name	Definition
Number of Ports	Choices are 1, 4, 8, 16, 32 and 48.
First Local Port No.	As indicated.
Local IP	Local IP address.
First Local TCP Port No.	As indicated.
Remote IP	Remote IP address.
First Remote TCP Port No.	As indicated.
Protocol	Communication method between master and slave (Telnet or SSH).

4. If you want to assign port names to the ports, select the **Port Names** button.

The system brings up the **Port Names** dialog box:



5. For each port to be named, enter the port name in the corresponding **Port Name** field, and then select the **OK** button.
6. Click on the **apply changes** button to save your configuration.

▼ **To Delete a Slave**

1. To delete a slave from the list, select the unit to be deleted from the Virtual Ports form, and then click **Delete**.

Ports Status

Show the status of each port. Information provided are: RS-232 signal status and which users are connected to each port.

Figure 4-48: Ports Status Form



Administration

System Information

System information provides information about the ACS version, CPU, memory, including PCMCIA.



Figure 4-49:System Information View

To view system information, select **Administration** from the top menu bar; select **System Information** from the left menu panel.

Notifications

The Notification form is used to set up alarm notification to users through email, pager or SNMP traps.

1. From the top menu bar, select **Administration**; from the left menu panel, select **Notifications**.

The system invokes the Notifications form:



Figure 4-50:Notifications Form

2. Complete the main form as follows:

Table 4-38: Notification Form Fields

Field Name	Definition
Notification Alarm for Data Buffering	Checkmark to enable notification alarms for data buffering.
[unlabeled view table]	List of alarm types and triggers.

Table 4-38: Notification Form Fields

Field Name	Definition
[<i>unlabeled dropdown list</i>]	Pull-down menu of notification methods (select: Email , Pager , or SNMP Trap).

3. Select the **Add** button.
4. The system brings up the Notifications Entry dialog box. The type of dialog box that appears will depend on the notification method that you select from the Notifications form.

Email Notifications

If you selected **Email** as the notification method, the following dialog box is used:

Figure 4-51: Email Notification Form

Table 4-39: Email Notification Form Fields

Field Name	Definition
Alarm Trigger <i>[untitled dropdown field]</i>	The trigger expression used to generate an alarm.
To/From/Subject/Body	The email for the designated recipient of the alarm notification.
SMTP Server IP	The IP address of the SMTP server.
SMTP Port	The port used by the SMTP server.

Pager Notifications

If you selected **Pager** as the notification method, the following dialog box is used:

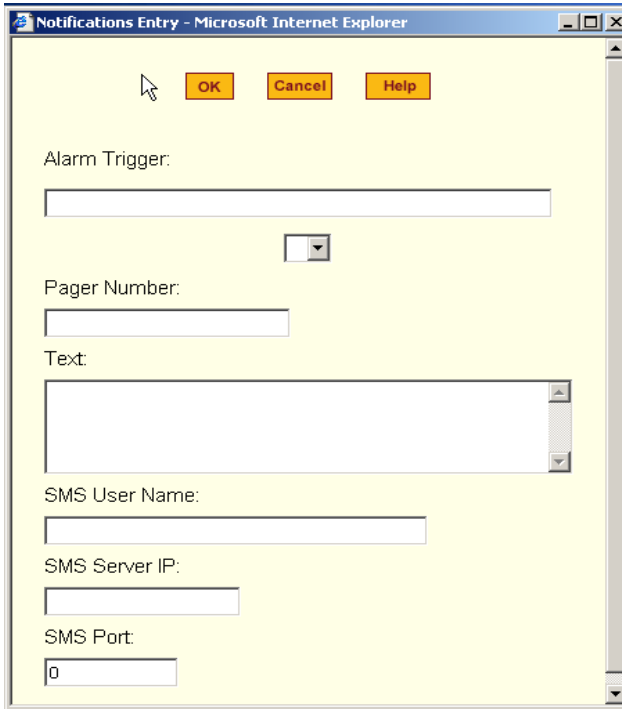


Figure 4-52: Pager Notification Form

Table 4-40: Pager Notification Form Fields

Field Name	Definition
Alarm Trigger [untitled dropdown field]	The trigger expression used to generate an alarm.
Pager Number	The pager number of the notification recipient.
Text	The text message for the pager.
SMS Server IP	The IP address of the SMS server.
SMS Port	The port used by the SMS server.

SNMP Trap Notifications

SNMP traps are event notifications that are sent to a list of managers configured to receive events for that managed system. The Traps provide the value of one or more instances of management information.

Any SNMP enabled Device generates Fault Reports (Traps) that are defined in the MIB (which the SNMP Agent has implemented).

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.

If you selected **SNMP Trap** as the notification method, the following dialog box is used:

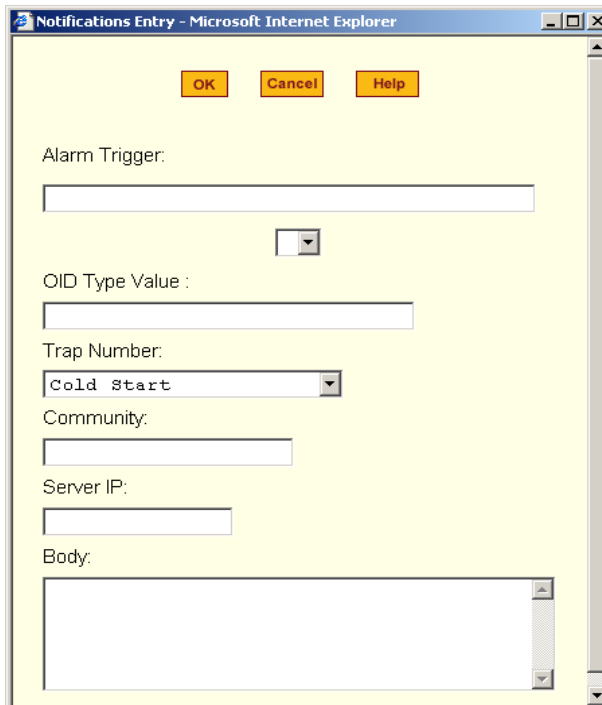


Figure 4-53:SNMP Notification Form

Table 4-41: SNMP Notification Form Fields

Field Name	Definition
Alarm Trigger	The trigger expression used to generate an SNMP trap. <i>[untitled dropdown field]</i>
OID Type Value	The value that uniquely identifies an object to the SNMP agent.
Trap Number	The trap type defined in the MIB.
Community	The password used to authenticate the traps
Server IP	The address of the server running the SNMP.
Body	The text or content of the notification.

1. Complete the **Notification Entry** dialog box, and select the **OK** button.
2. Select the **apply changes** button at the bottom of the ACS configuration window to save your configuration.

Port Alarm Notification

You can configure the Notification form to monitor the DCD signal such that the system will generate an alarm in any of the following events:

- A serial console cable is removed from the console server
 - A server/network equipment attached to the console is powered down.
 - The configuration also enables you to detect if a modem that is in use is still powered on and active.
1. From the Notification form, select the Action (Email, SNMP Trap or Pager).
 2. Click the Add button.
 3. Enter the Alarm Trigger: Port
 4. Configure the parameters of the action
 5. Select Apply Changes

Time / Date

The Time/Date form is used to enable ACS to work as an NTP client. Network Time Protocol (NTP) is a standard for synchronizing your system clock with the *true time*, defined as the average of many high-accuracy clocks around the world. By default, NTP is disabled and you may enter the time and date manually using the Time/Date form.

Manual Setting

To set the time and date manually (*i.e.*, locally, without NTP), perform the following steps:

1. Select **Administration** from the top menu bar, and then select **Time/Date** from the left menu panel.

The system brings up the **Time/Date** form:

The screenshot shows the 'Time/Date' configuration page in the ACS web interface. The interface has a yellow and orange theme. At the top, there is a navigation bar with 'Applications | Network | Security | Ports | Administration'. On the right, it shows 'Host Name: CAS', 'IP Address: 192.168.46.72', and 'Model: ACS4'. A 'logout' link is in the top right corner. On the left, a sidebar menu includes 'System Information', 'Notifications', 'Time / Date' (highlighted), 'Boot Configuration', 'Backup Config', 'Upgrade Firmware', and 'Reboot'. The main content area is titled 'Network Time Protocol' with a dropdown menu set to 'Disable'. Below this, there are two sections: 'Date' and 'Time'. The 'Date' section has input fields for 'Month' (5), 'Day' (12), and 'Year' (2004). The 'Time' section has input fields for 'Hour' (15), 'Minute' (19), and 'Second' (29). At the bottom, there is a 'Wizard' button and a row of control buttons: 'try changes', 'cancel changes', 'apply changes', 'reload page', 'Help', and 'no unsaved changes'.

Figure 4-54: Time/Date Form

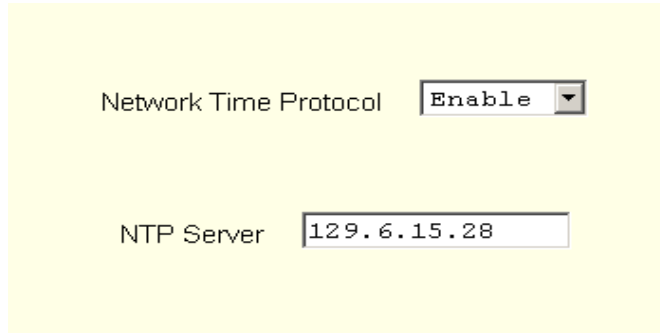
2. If you are not using NTP, complete the date and time fields by selecting the appropriate numbers from the dropdown list boxes.
3. Click on the **Apply Changes** button to complete the procedure.

Setting Network Time Protocol (NTP)

To set the time and date through NTP, perform the following steps:

Configuring the ACS in Expert Mode

1. From the Time/Date form, choose **Enable** from the **Network Time Protocol** field.
2. Type in the address of the NTP server in the **NTP Server** field.



The screenshot shows a configuration form with two fields. The first field is labeled "Network Time Protocol" and has a dropdown menu with "Enable" selected. The second field is labeled "NTP Server" and contains the IP address "129.6.15.28".

3. Click on the **Apply Changes** button.

Boot Configuration

Boot configuration defines the settings for loading the operating system. In the event that the ACS fails to boot successfully, you can use the Boot Configuration form to change the boot settings.

The ACS can boot from its internal firmware or from the network. By default, the unit boots from Flash. If you need to boot from the network, install one TFTP or BOOTP server with the firmware to boot from, and then choose **boot from network** and fill in the fields. You may skip Flash test and RAM test for a faster boot.

1. From the top menu, select **Administration**; from the left menu, select **Boot Configuration**.

The system brings up the Boot Configuration form:

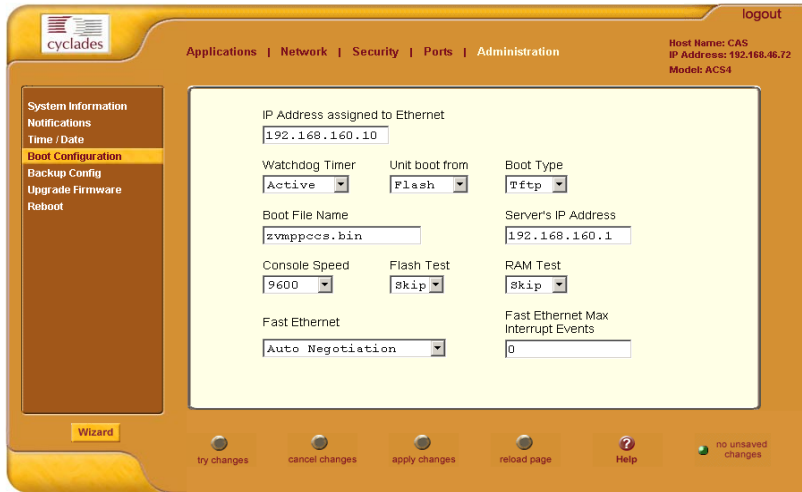


Figure 4-55: Boot Configuration Form

2. Complete the fields as follows:

Table 4-42: Boot Configuration Form Fields

Field Name	Definition
IP Address assigned to Ethernet	As indicated.
Watchdog Timer	Sets the Watchdog Timer to Active or Inactive.
Unit boot from	Specify whether to boot unit up from Flash or from the.
Boot Type	Select from the following types of booting: bootp, tftp, or both.
Boot File Name	Filename of the boot program you want to use.
Server's IP Address	As indicated.
Console Speed	Select from: 4800 through 118200.
Flash Test	Select this to test boot from the Flash card. You can Skip this test, or do a Full test.

Table 4-42: Boot Configuration Form Fields

Field Name	Definition
RAM Test	Select this to test boot from RAM. You can Skip this test, do a Quick test or a Full test.
Fast Ethernet	Select the appropriate Ethernet setting if you need to change the Auto Negotiation (default value): 100BaseT Half-Duplex 100BaseT Full-Duplex 10BaseT Half-Duplex 10BaseT Full-Duplex
Fast Ethernet Max. Interrupt Events	The maximum number of packets that the CPU will handle.

3. Select **Apply Changes** to save your configuration to Flash.

Backup Configuration

The Backup Configuration form allows you to:

- Use a FTP server to save and retrieve your ACS configuration. For the backup configuration to work, the FTP server must be on the same subnet. Ensure that it is accessible from the ACS by pinging the FTP server.
- Use a storage device to save your configuration.

▼ *To save configuration to an FTP server*

1. From the top menu, select **Administration**; from the left menu, select **Backup Configuration**.

The system brings up the **Backup Configuration** form:



Figure 4-56: Backup Configuration Form

2. Complete the form as follows:

Table 4-43: Backup Configuration Form Fields

Field Name	Definition
Type	Type of backup: FTP or Storage Device.
Server IP	IP address of the FTP server.
Path and Filename	Path and filename of the FTP server.
Username	Username of the person who is doing the backup.
Password	Password associated with the Username.

Note: Read the succeeding section, **Backup and Restore Procedure**, for a more detailed explanation of the fields.

3. Select **Save to FTP Server** or **Upload from FTP Server**, as appropriate.

▼ **Backup and Restore Procedure**

For backup purposes, you can give the configuration backup file a name according to your company's naming convention.

From the Backup Configuration form, fill in the fields with the server name (*i.e.*, the IP address of your workstation if you have just installed an FTP server in it), Username and Password (for a valid username defined in your FTP server), and the Path and Filename to which you have rights to access and write. The **Path** and **Filename** field must contain the full path and the filename that you will assign to the backup file.

Example:

To upload to the upload folder with the filename, AcsxxxxConfig040521, type in the following in the **Path and Filename** field:

```
upload/AcsxxxxConfig040521
```

Always check the FTP server's upload folder after you have selected the **Save to FTP Server button**. Ensure that the file is there as some FTP servers do not return error conditions, which can cause the ACS to display a "DONE" result even though the FTP did not store a copy.

▼ **To Save Configuration to a Storage Device**

Note: For this feature to work, the **RESTORECONF** utility must be modified to enable the system to read the configuration file from the compact flash. *Refer to the ACS Advanced Administration Guide for more details.*

1. From the top menu, select **Administration**; from the left menu, select **Backup Configuration**.
2. From the **Type** dropdown field of the Backup Configuration form, select **Storage Device**.

The system displays the following form:



Figure 4-57: Backup Configuration Form (Storage Device)

3. Complete the form as follows:

Table 4-44: Backup Configuration Form Fields (Storage Device)

Field Name	Definition
Default Configuration	The system uses the configuration in the storage device but does not override the internal flash configuration after reboot.
Replace Configuration	The system saves the configuration in the storage device with a flag REPLACE that is used by the RESTORECONF utility.

4. Click on **Save**.
5. Click on **Apply Changes**.

Upgrade Firmware

The Upgrade Firmware form allows you to upload the ACS firmware from the Cyclades website to the ACS. To upgrade the ACS firmware, follow the procedure below:

Configuring the ACS in Expert Mode

1. Select **Administration** from the top menu, and then select **Upgrade Firmware** from the left menu.

The system brings up the **Upgrade Firmware** form:

Figure 4-58: Upgrade Firmware Form

2. Complete the form as follows:

Table 4-45: Upgrade Firmware Form Fields

Field Name	Definition
Type	The method of upload.
FTP Site	The address of the FTP site.
Username	Username of the person who is doing the upload.
Password	Password associated with the Username.
File Version	The firmware file version.
Run Checksum	Runs the checksum program to verify the accuracy of the uploaded data.

3. Click on **Upgrade Now**.

Reboot

The Reboot form allows you to reboot the system by clicking the Reboot button.



Figure 4-59: Reboot Window

Appendix A

Hardware Specifications

The following table lists the AlterPath Advanced Console Server hardware specifications

CPU	MPC855T (PowerPC Dual-CPU)
Memory	128MB DIMM SDRAM / 16MB CompactFlash
Interfaces	1 Ethernet 10/100BT on RJ45 1 RS232 Console on RJ45 RS232 Serial Ports on RJ45 PCMCIA slots supporting: Secondary Ethernet, Wireless networking, CDMA, GPRS, GSM, V.90 modems, ISDN
Power	Internal 100-240VAC, 50/60 Hz† Optional Dual entry, redundant power supplies† † -48VDC option available
Operating Temperature	50°F to 112°F (10°C to 44°C)
Storage Temperature	-40°F to 185°F (-40°C to 85°C)
Humidity	5% to 90% non-condensating
Dimensions	ACS1: 6.3 x 4.0 x 1.5 in (16 x 10 x 3.8 cm) ACS 4-48: 17 x 8.5 x 1.75 in (43.18 x 21.59 x 4.45 cm)
Certification	FCC Part 15, A EN55022, A (CE) EN55024 UL 1950 Solaris Ready™

Appendix B

Safety Guidelines

The following Safety Guidelines for AlterPath Advanced Console Server are described in this appendix.

Safety Guidelines for Rack-Mounting the Advanced Console server	Page 142
Safety Precautions for Operating the Advanced Console server	Page 143
Working inside the AlterPath Advanced Console Server	Page 144
Replacing the Battery	Page 144
FCC Warning Statement	Page 144
Notice About FCC Compliance for all Alterpath Advanced Console Server Models	Page 145
Canadian DOC Notice	Page 145
Aviso de Precaución S-Mark Argentina	Page 145
Trabajar dentro del AlterPath Advanced Console Server	Page 146
Batería	Page 146

Safety Guidelines for Rack-Mounting the ACS

The following considerations should be taken into account when rack-mounting the AlterPath Advanced Console Server.

Temperature

The manufacturer's maximum recommended ambient temperature for the AlterPath Advanced Console Server is 122 °F (50 °C).

Elevated Operating Ambient Temperature

If the ACS is installed in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than room ambient temperature. Therefore, consideration should be given to installing the equipment in an environment compatible with the manufacturer's maximum rated ambient temperature. See above.

Reduced Air Flow

Installation of the equipment in a rack should be such that the amount of air flow required for safe operation of the equipment is not compromised.

Mechanical Loading

Mounting of the equipment in the rack should be such that a hazardous condition is not achieved due to uneven mechanical loading.

Circuit Overloading

Consideration should be given to the connection of the equipment to the supply circuit and the effect that overloading of circuits might have on overcurrent protection and supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing this concern.

Reliable Earthing

Reliable earthing of rack-mounted equipment should be maintained. Particular attention should be given to supply connections other than direct connections to the branch circuit, such as power strips or extension cords.

Safety Precautions for Operating the ACS

Please read all the following safety guidelines to protect yourself and your AlterPath Console Server.

Caution: Do not operate your ACS with the cover removed.

Caution: To avoid shorting out your ACS when disconnecting the network cable, first unplug the cable from the Host Server, unplug external power (if applicable), equipment and then unplug the cable from the network jack. When reconnecting a network cable to the back equipment, first plug the cable into the network jack, and then into the Host Server equipment.

Caution: To help prevent electric shock, plug the ACS into a properly grounded power source. The cable is equipped with a three-prong plug to help ensure proper grounding. Do not use adapter plugs or remove the grounding prong from the cable. If you have to use an extension cable, use a three-wire cable with properly grounded plugs.

Caution: To help protect the ACS from electrical power fluctuations, use a surge suppressor, line conditioner, or uninterruptible power supply. Be sure that nothing rests on the cables of the ACS and that they are not located where they can be stepped on or tripped over. Do not spill food or liquids on the ACS.

Caution: Do not push any objects through the openings of the ACS. Doing so can cause fire or electric shock by shorting out interior components.

Caution: Keep your ACS away from heat sources and do not block host's cooling vents.

Caution: The AlterPath Console Server product (DC version) is only intended to be installed in restricted access areas (Dedicated Equipment Rooms, Equipment Closets or the like) in accordance with Articles 110-18, 110-26 and 110-27 of the National Electrical Code, ANSI/NFPA 701, 1999 Edition. Use 18 AWG or 0.75 mm² or above cable to connect the DC configured unit to the Centralized D.C. Power Systems. Install the required double-pole, single-throw, DC rated UL Listed circuit breaker between the power source and the AlterPath Console Server DC version. Minimum Breaker Rating: 2A. Required conductor size: 18 AWG.

Working inside the AlterPath Console Port Server

Do not attempt to service the AlterPath Advanced Console Server yourself, except when following instructions from Cyclades Technical Support personnel. In the latter case, first take the following precautions:

1. Turn the AlterPath Advanced Console Server off.
2. Ground yourself by touching an unpainted metal surface on the back of the equipment before touching anything inside it.

Replacing the Battery

Caution: There is the danger of explosion if the battery is replaced incorrectly. Replace the battery only with the same or equivalent type recommended by the manufacturer. Dispose of used batteries according to the manufacturer's instructions.

Vorsicht: Bei Einsetzen einer falschen Batterie besteht Explosionsgefahr. Ersetzen Sie die Batterie nur durch den gleichen oder vom Hersteller empfohlenen Batterietyp. Entsorgen Sie die benutzten Batterien nach den Anweisungen des Herstellers.

FCC Warning Statement

The AlterPath Advanced Console Server has been tested and found to comply with the limits for Class A digital devices, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment.

This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the Installation & Service Manual, may cause harmful interference to radio communications.

Operation of this equipment in a residential area is likely to cause harmful interference in which case the user is required to correct the problem at his or her own expense.

Notice About FCC Compliance for all Alterpath ACS Models

To comply with FCC standards, the AlterPath Advanced Console Server require the use of a shielded CAT 5 cable for the Ethernet interface. Notice that this cable is not supplied with either of the products and must be provided by the customer.

Canadian DOC Notice

The AlterPath Advanced Console Server does not exceed the Class A limits for radio noise emissions from digital apparatus set out in the Radio Interference Regulations of the Canadian Department of Communications.

L'AlterPath Advanced Console Server n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de la classe A prescrites dans le règlement sur le brouillage radioélectrique édicté par le Ministère des Communications du Canada.

Aviso de Precaución S-Mark Argentina

Por favor de leer todos los avisos de precaución como medida preventiva para el operador y el AlterPath Advanced Console Server.

precaución:No hacer funcionar el AlterPath Advanced Console Server con la tapa abierta.

precaución:Para prevenir un corto circuito en el AlterPath Advanced Console Server al desconectarlo de la red, primero desconectar el cable del equipo y luego el cable que conecta a la red. Para conectar el equipo a la red, primero conectar el cable a la red y luego al equipo.

precaución:Asegurarse que el equipo este conectado a tierra, para prevenir un shock eléctrico. El cable eléctrico del equipo viene con tres clavijas para conectar asegurar conexión a tierra. No use adaptadores o quite la clavija de tierra. Si se tiene que utilizar una extensión, utilice una que tenga tres cables con clavija para conexión a tierra. Para proteger al AlterPath Advanced Console Server de fluctuaciones en corriente eléctrica, utilice una fuente eléctrica de respaldo. Asegurarse de que nada descansa sobre los cables del AlterPath Advanced Console Server, y que los cables no obstruyan el paso. Asegurarse de no dejar caer alimentos o bebidas en el AlterPath Advanced Console Server. Si esto ocurre, avise a Cyclades Corporation.

precaución:No empuje ningún tipo de objeto en los compartimientos del AlterPath Advanced Console Server. Hacer esto podría ocasionar un incendio o causar un corto circuito dentro del equipo.

precaución:Mantenga el AlterPath Advanced Console Server fuera del alcance de calentadores, y asegurarse de no tapar la ventilación del equipo.

precaución:El AlterPath Advanced Console Server con alimentación de corriente directa (CD) solo debe ser instalado en áreas con restricción y de

acuerdo a los artículos 110-18, 110-26, y 110-27 del National Electrical Code, ANSI/NFPA 701, Edición 1999. Para conectar la corriente directa (CD) al sistema, utilice cable de 0.75 mm (18 AWG). Instalar el interruptor corriente directa (CD) aprobado por UL entre la fuente de alimentación y el AlterPath Advanced Console Server. El límite mínimo del interruptor deberá ser 2 amperes, con conductor de 0.75 mm (18 AWG).

Trabajar dentro del AlterPath Advanced Console Server

No intente dar servicio al AlterPath Advanced Console Server, solo que este bajo la dirección de Soporte Técnico de Cyclades. Si este es el caso, tome las siguientes precauciones:

Apague el AlterPath Advanced Console Server. Asegurase que este tocando tierra antes de tocar cualquier otra cosa, que puede ser al tocar la parte trasera del equipo.

Batería

precaución: Una batería nueva puede explotar, si no esta instalada correctamente. Reemplace la batería cuando sea necesario solo con el mismo tipo recomendado por el fabricante de la batería. Deshacerse de la batería de acuerdo a las instrucciones del fabricante de la batería.

Appendix C

Supported Browsers and JRE

The following are the list of topics that are covered in this appendix.

- AlterPath ACS supported browsers
- Java Runtime Environment (JRE) requirements
- JRE installation procedures
 - Using Windows and Internet Explore browser
 - Using Windows and Netscape or Mozilla browsers

Supported Web Browsers

The web browsers that support the AlterPath Console Server web interface are as follows:

- Netscape 7.1 for Windows
- Mozilla 1.3a for Windows
- MS Internet Explorer 6.0

Browsers that do not support the ACS web interface:

- Netscape Communicator 4.8
- Netscape Communicator 4.79

Installing JRE

Tested Environments

- Windows XP + JREv1.4.2.
- Internet Explorer 6.0 Successful
- Netscape 6.0 - 6.2.3 Successful
- Netscape 7.0 - 7.1 Successful
- Mozilla 1.1 - 1.3a Successful

Installation Requirements

For the ACS application to run, you must have Java 2 Runtime Environment (JRE) version 1.4.2. (which can be found at <http://java.sun.com/>) installed on your PC with your browser acknowledged to use it. You can first check if the browser you are using acknowledges the Java version by following the procedures given in the next sections.

Installing From Windows Internet Explorer

Go to **Tools > Internet Options > Advanced**. Scroll down and look for a section on Java. There should be a check box that says "Use Java 2 v1.4.2...." If there isn't, this could either mean your browser is not activated to use the Java plug-in that came with the JRE you have installed or it just means that you don't have any JRE installed, in which case please install and repeat the check.

If you have already installed JRE and you just want to activate your browser to use it, go to your system's Control Panel > Java Plug-in icon > Browser > check on the browser(s) you want to activate to use the Java Plug-in. Now repeat the check to see if your browser will now use the correct Java Plug-in.

Installing From Windows Netscape or Mozilla

Check to see if Java is enabled. Go to Edit > Preferences > Advanced > Check on Enable Java. To see what version of JRE Plug-in is used, go to Help > About Plug-ins. Scroll down to Java Plug-in section. Check if the Java Plug-in is the version you have installed.

TIP: When installing Netscape 7.0, it will ask if you want to install Sun Java. If you click on the box to install it, a version of JRE will be installed into your system; however, this does not mean that other browsers such as IE will recognize it. If you choose not to install Sun Java through Netscape but do it separately, Netscape 7.0 should automatically detect the JRE, and this can be checked by the instructions mentioned above.

Glossary

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.

Bonding (Linux)

Ability to detect communication failure transparently, and switch from one LAN connection to another. The Linux bonding driver has the ability to detect link failure and reroute network traffic around a failed link in a manner transparent to the application. It also has the ability (with certain network switches) to aggregate network traffic in all working links to achieve higher throughput. The bonding driver accomplishes this by enslaving all of the Ethernet ports in the bond to the same Ethernet MAC address, which ensures the proper routing of packets across the links.

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).
Break Signal	A break signal is generated in an RS-232 serial line by keeping the line in zero for longer than a character time. Breaks at a serial console port are interpreted by Sun servers as a signal to suspend operation and switch to monitor mode.
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.
Cluster	A cluster is a group of one or more computers working as a group to execute a certain task. From the user standpoint, a cluster acts as a large computer system.
Console Access Server (CAS)	A CAS has an Ethernet LAN connection and many RS-232 serial ports. It connects to the console ports of servers and networking equipment and allows convenient and secure access from a single location.
Community	The community name acts as a password and is used 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.
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.
Console Port	Most of the equipment in a data center (servers, routers, switches, UPS, PBX, etc.) has a serial console port for out-of-band management purposes.

DHCP

Dynamic Host Configuration Protocol. A protocol for automatic TCP/IP configuration that provides static and dynamic address allocation and management.

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.

DNS Server

Domain Name Server. The computer you use to access the DNS to allow you to contact other computers on the Internet. The server keeps a database of host computers and their IP addresses.

Domain Name

The unique name that identifies an Internet site. Domain Names always have 2 or more parts, separated by dots. The part on the left is the most specific, and the part on the right is the most general. A given machine may have more than one Domain Name but a given Domain Name points to only one machine. For example, the domain names: matisse.net, mail.matisse.net, workshop.matisse.net can all refer to the same machine, but each domain name can refer to no more than one machine. Usually, all of the machines on a given Network will have the same thing as the right-hand portion of their Domain Names (matisse.net in the examples above). It is also possible for a Domain Name to exist but not be connected to an actual machine. This is often done so that a group or business can have an Internet e-mail address without having to establish a real Internet site. In these cases, some real Internet machine must handle the mail on behalf of the listed Domain Name.

Escape Sequence

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.

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 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.

FTP

Short for *File Transfer Protocol*. The protocol for exchanging files over the Internet. FTP works in the same way as HTTP for transferring web pages from a server to a user's browser. FTP uses the Internet's TCP/IP protocols to enable data transfer.

Hot-Swap

Ability to remove and add hardware to a computer system without powering off the system.

ICMP	<i>Internet Control Message Protocol</i> is an Internet protocol sent in response to errors in TCP/IP messages. It is an error reporting protocol between a host and a gateway. ICMP uses Internet Protocol (IP) datagrams (or <i>packets</i>), but the messages are processed by the IP software and are not directly apparent to the application user.
In-band Network Management	In a computer network, when the management data is accessed using the same network that carries the data, this is called “in-band management.”
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.
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 for 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.
ISDN	A set of communications standards allowing a single wire or optical fibre to carry voice, digital network services and video. ISDN is intended to eventually replace the plain old telephone system.

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.

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.

Masquerading

Where a system acts on behalf of other systems, such as when an ISP server accesses network services on behalf of a dial-up user.

MTU

Short for *Maximum Transmission Unit*, the largest physical packet size, measured in bytes, that a network can transmit. Any messages larger than the MTU are divided into smaller packets before being sent.

Every network has a different MTU, which is set by the network administrator. On Windows, you can set the MTU of your machine. This defines the maximum size of the packets sent from your computer onto the network. Ideally, you want the MTU to be the same as the smallest MTU of all the networks between your machine and a message's final destination. Otherwise, if your messages are larger than one

of the intervening MTUs, they will get broken up (fragmented), which slows down transmission speeds.

Trial and error is the only sure way of finding the optimal MTU, but there are some guidelines that can help. For example, the MTU of many PPP connections is 576, so if you connect to the Internet via PPP, you might want to set your machine's MTU to 576 too. Most Ethernet networks, on the other hand, have an MTU of 1500.

Network Mask

A 32-bit number used to group IP addresses together or to indicate the range of IP addresses on a single IP network/subnet/supernet. There is a group of addresses assigned to each network segment. For example, the mask 255.255.255.0 groups together 254 IP addresses. If we have, as another example, a sub-network 192.168.16.64 with mask 255.255.255.224, the addresses we may assign to computers on the sub-network are 192.168.16.65 to 192.168.16.94, with a broadcast address of 192.168.16.95.

A number used by software to separate the local subnet address from the rest of a given Internet protocol address

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.

NFS

Network File System is a protocol suite developed and licensed by Sun Microsystems that allows different makes of computers running different operating systems to share files and disk storage. NFS is implemented using a connectionless protocol (UDP) in order to make it stateless.

NTP *Network Time Protocol.* A standard for synchronizing your system clock with the "true time", defined as the average of many high-accuracy clocks around the world.

Object Identifiers (OID) The SNMP manager or the management application uses a well-defined naming syntax to specify the variables to the SNMP agent. Object names in this syntax are called Object Identifiers (Object IDs or OIDs). OIDs are series of numbers that uniquely identify an object to an SNMP agent. OIDs are arranged in a hierarchical, inverted tree structure.

The OID tree begins with the root and expands into branches. Each point in the OID tree is called a node and each node will have one or more branches, or will terminate with a leaf node. The format of OID is a sequence of numbers with dots in between.

There are two roots for Object Identifiers, namely iso and ccit. iso starts with.1 and ccit starts with.0. Most Object Identifiers start with.1.3.6.1, where 1=iso, 3=org, 6= dod, 1 = internet. The Internet sub-tree branches into mgmt and private.

To understand the concept of relative and absolute Object Identifiers, let us consider the AdventNet Object Identifier.1.3.6.1.4.1.2162. It specifies the path from the root of the tree. The root does not have a name or a number but the initial 1 in this OID is directly below root. This is called an absolute OID. However, a path to the variable may be specified relative to some node in the OID tree. For example, 2.1.1.7 specifies the sysContact object in the system group, relative to the Internet (.1.3.6.1) node in the OID tree. This is called a relative OID.

Off-Line Data Buffering This is a CAS feature that allows capture of console data even when there is no one connected to the port.

OID See **Object Identifier**.

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

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.

The following lists the available parity parameters and their meanings:

Odd - Parity bit set so that there is an odd number of 1 bits

Even - Parity bit set so that there is an even number of 1 bits

None - Parity bit is ignored, value is indeterminate

PCMCIA

Personal Computer Memory Card International Association. An organization consisting of some 500 companies that has developed a standard for small, credit card-sized devices, called PC Cards. Originally designed for adding memory to portable computers, the PCMCIA standard has been expanded several times and is now suitable for many types of devices including network cards (NICs).

The PCMCIA 2.1 Standard was published in 1993. As a result, PC users can be assured of standard attachments for any peripheral device that follows the standard.

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 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.

Profile

Usage setup of the ACS either as a Console Access Server (CAS), a Terminal Server, or a Remote Access Server.

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.

RISC

Reduced Instruction Set Computer. This describes a computer processor architecture that uses a reduced set of instructions (and achieves performance by executing those instructions very fast.) Most UNIX servers (Sun Sparc, HP, IBM RS6000, Compaq Alpha) were designed with a processor using a RISC architecture. The Intel[®] x86 architecture.

Root Access

Root is the term for a very highly privileged administrative user (particularly in unix environments). When an ISP grants you root access, it means you will have full control of the

server. With full control, you will be able to install any software and access any file on that server.

Routing Table

The Routing Table defines which interface should transmit an IP packet based on destination IP information.

RPC

Short for *Remote Procedure Call*. A type of protocol that allows a program on one computer to execute a program on a server. Using RPC, a system developer do not need to develop specific procedures for the server. The client program sends a message to the server with appropriate arguments and the server returns a message containing the results of the program executed.

Secure Shell (SSH)

SSH has the same functionality as Telnet (see definition for **Telnet**), but adds security by encrypting data before sending it through the network.

Server Farm

A collection of servers running in the same location (see **Cluster**).

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

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.

Any SNMP enabled Device generates Fault Reports (Traps) that are defined in the MIB (which the SNMP Agent has implemented).

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.

Stop Bit

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.

Subnet Mask

A bit mask used to select bits from an Internet address for subnet addressing. Also known as Address Mask.

SSH (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.

STTY

Set the options for a terminal device interface.

This command prints information about your terminal settings. The information printed is the same as if you had typed stty while interacting with a shell.

The stty utility sets or reports on terminal I/O characteristics for the device that is its standard input. Without options or operands specified, it reports the settings of certain characteristics, usually those that differ from implementation-dependent defaults. Otherwise, it modifies the terminal state according to the specified operands.

TACACS

Terminal Access Controller Access Control System.
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.

TACACS+

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.

TCP Keep-Alive Interval

The time interval between the periodic polling of all inactive TCP/IP connections, checking that the client processes really are still there. After a certain period of inactivity on an established connection, the server's TCP/IP software will begin to send test packets to the client, which must be acknowledged. After a preset number of 'probe' packets has been ignored by the client, the server assumes the worst and the connection is closed.

The keep-alive timer provides the capability to know if the client's host has either crashed and is down or crashed and rebooted.

Telnet

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 executed as if you were entering them directly on the server console

Terminal Server

A terminal server has one Ethernet LAN port and many RS-232 serial ports. It is used to connect many terminals to the network. Because they have the same physical interfaces, terminal servers are sometimes used as console access servers.

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.

U Rack Height Unit

A standard computer rack has an internal width of 17 inches. Rack space on a standard rack is measured in units of height (U). One U is 1.75 inches. A device that has a height of 3.5 inches takes 2U of rack space.

VPN

Virtual Private Networking allows local area networks to communicate across wide area networks, typically over an encrypted channel. See also: **IPsec**.

Watchdog Timer

A watchdog timer (WDT) is a device or electronic card that performs a specific operation after a certain period of time if something goes wrong with an electronic system and the system does not recover on its own.

A common problem is for a machine or operating system to lock up if two parts or programs conflict, or, in an operating system, if memory management trouble occurs. In some cases, the system will eventually recover on its own, but this may take an unknown and perhaps extended length of time.

A watchdog timer can be programmed to perform a warm boot (restarting the system) after a certain number of seconds during which a program or computer fails to respond following the most recent mouse click or keyboard action.

The timer can also be used for other purposes, for example, to actuate the refresh (or reload) button in a Web browser if a Web site does not fully load after a certain length of time following the entry of a Uniform Resource Locator (URL).

Index

A

- Access Configuration, Wizard Mode 45
- Access form, Ports 111
- Access Method
 - Compact Flash 77
 - Ethernet 76
 - GSM 76
 - ISDN 75
 - Modem 74
 - Wireless LAN 78
- Access to ACS 39
- Access to Serial Ports 40
- ACS firmware 138
- Active Port Sessions 102
- add 81
- Add/Edit User dialog box 62
- Adding a Chain 88
- Adding a Rule 94
- Adding Users and Groups to the Access List 100
- Administration 125
- Allow Multiple Sessions 118
- AlterPath ACS Login page 32
- Apply Changes button 37
- Authentication
 - LDAP or LdapDownLocal 114
 - Radius 114
- Authentication Method, VPN 81
- Authentication Protocol, VPN 81
- Authentication Type

Kerberos, KerberosDownLocal 114
NIS, LocalNIS or NISLocal 114

B

Backup and Restore Procedure 137
Backup Configuration form 135
Baud Rate 45
Bonding 70, 155
 miimon 70
 updelay 70
Boot Configuration 133
boot from network 133
boot settings 133
brackets, mounting 9
Buffer to Syslog 115
Button Functions 36

C

Chain 87
Changing a User Password 47
Changing the User Password 101
Clear Max Detected Current 61
Clear Max Detected Temperature 61
Closing the session from ts_menu 26
COM port 15
Compact Flash 74
Configure PCMCIA Cards 72
Configure the Security Settings 40
Configure User Access to Serial Ports 46
Configure VPN Connections 80
Configuring in Expert Mode 53
Connecting to a port 56
Connection Protocol, Port Profile 45
Console Access Profile (CAS) 43
console port

D

- Data Buffering 106, 115
- Data Size, Port Profile 45
- DB-9 connector 8
- Deleting a Chain 89
- Deleting a Slave 122, 124
- Deleting a User from a Group 101
- Deleting a User, Power Management 63
- Deleting a User, Wizard Mode 49
- DHCP, network settings 68
- document
 - related documentation vii
- Documentation CD 6

E

- edit 80
- Edit Rule dialog box 90
- Editing a Chain 88
- Editing a Rule 89
- Email Notification 127
- Enable Data Buffering, Ports configuration 115
- escape character 26
- Ethernet 8, 74
- Expert Mode 35
- Expert Mode Menu 53

F

- Firewall configuration 86
- Flow Control, Port Profile 45
- FreeSWAN 79
- FTP 40

G

General form, Ports 108

GSM 74

H

Hardware Specifications vi

Host Tables form 95

HyperTerminal 12

I

ICMP 40

ICMP Options 93

Initial Configuration Using the ACS Console Port 14

installation and configuration process 13

IP filtering 86

IPDU 8

IPSec 40

IPsec tunnels 79

ISDN 74

J

Java 2 JRE 12

Java window 24

JCPU 103

JRE vi

K

Kerberos 112

kerberosDownLocal 112

Kermit 12

L

- LAN 8
- launch an SSH session 66
- Ldap 112
- ldapDownLocal 113
- Local/Radius 112
- Local/TacacsPlus 112
- Logging In, Web User Interface 32
- Login Banner 121

M

- Miimon 70
- Minicom 12
- Modem 74
- modify selected ports 107
- mounting
 - brackets 9
- Multi User 106
- Multi User form 116

N

- Net-SNMP package 82
- Network Host Settings 68
- Network Settings 41
- New/Modify Host dialog box 96
- New/Modify Route dialog box 98
- New/Modify SNMP v3 Configuration dialog box 86
- New/Modify VPN Connection dialog box 81
- NIS NIS 113
- Notification Alarm for Data Buffering 126
- Notifications form 126
- NTP client 132
- NTP Setting 132

O

OID 83

Outlets Manager form 58, 60

P

Package Contents 6

Pager Notifications 129

Parameters for All Serial Ports 44

Parity, Port Profile 45

PCMCIA card 74

PCMCIA Configuration Dialog Boxes 74

PCMCIA Management form 72

PCPU 103

Physical Ports form 106

plugs 7

Port Profile form 44

Port profile, 43

Ports configuration 106

Power Management 27

Power Management Configuration 64

Power management form 57

Power Up Interval field 60

Q

QuickStart 6

R

Rack Mounting the ACS 10

Radius 112

Radius/Local 112

RadiusDownLocal 112

Reboot button 140

Reboot form 140

- Reject Options 94
- RJ-45 to DB-9 adapter, female cross converter 8
- RJ-45 to RJ-45 cable 8
- RPC 40
- RSA Key, VPN 82
- Rule 87
- Run Checksum 139

S

- Safety vi
- Safety Guidelines 143
- Saving Your Configuration 37
- Security 28
- Security configuration 99
- Security profile 38
 - custom 39
 - default 39
 - moderate 39
 - open 39
 - secured 39
- Security Settings 40
- serial ports 8
- Services 40
- Sniff Mode 118
- SNMP 40, 82
- SNMP Daemon Settings 82, 83
- SNMP Trap Notification 130
- SNMPv1, v2 and v3 83
- SNMPv1/v2 83
- SNMPv3 85
- Software Upgrade, Power Management 64
- SSH Access 25
- Static Routes form 97
- Stop Bits, Port Profile 45
- STTY Options 121
- Syslog form 71

T

- TacacsPlus 112
- TacacsPlus/Local 112
- TacacsPlusDownLocal 112
- Telnet Access 25
- Terminal Profile Menu 65
- Test Configuration 19
- Time/Date form 132
- To 28
- to change your password 28
- ts_menu Access 26
- TTY 102

U

- United 7
- United States
 - power cord for 7
- Unsaved Changes indicator 37
- Updelay 70
- Upgrade Firmware form 138
- Users and Groups configuration 99
- Using the Command Line Interface (CLI) 24
- Using the Web Interface 22

V

- Virtual Ports form 121
- Virtual Private Network 79
- VPN 78, 79
- VPN configuration form 80

W

- Watchdog Timer 134
- Wireless LAN 74

Wizard Mode 34