We believe the information in this manual is accurate and reliable. However, we assume no responsibility, financial or otherwise, for any consequences of the use of this product or manual. This manual is published by Cyclades Corporation, which reserves the right to make improvements or changes in the products described in this manual as well as to revise this publication at any time and without notice to any person of such revision or change. The operating system covered in this manual is v2.3.0. All brand and product names mentioned in this publication are trademarks or registered trademarks of their respective holders.

Cyclades, AlterPath ACS1, AlterPath ACS4, AlterPath ACS8, AlterPath ACS16, AlterPath ACS32, and AlterPath ACS48 are registered trademarks of Cyclades Corporation. Microsoft, Windows 95, 98, XP, ME, NT, and 2K are trademarks of Microsoft Corporation. UNIX is a trademark of UNIX System Laboratories, Inc. Linux is a registered trademark of Linus Torvalds.

For latest manual revisions, please refer to Cyclades website on: http://www.cyclades.com/support/downloads.php

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, 41829 Albrae Street, Fremont, CA 94538, USA. Telephone (510) 771-6100. Fax (510) 771-6200. www.cyclades.com.
# Table of Contents

## Before You Begin

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audience</td>
<td>1</td>
</tr>
<tr>
<td>Document Organization</td>
<td>1</td>
</tr>
<tr>
<td>Typographical Conventions</td>
<td>2</td>
</tr>
<tr>
<td>Naming Conventions</td>
<td>3</td>
</tr>
<tr>
<td>Document Symbols</td>
<td>4</td>
</tr>
<tr>
<td>Cross References</td>
<td>4</td>
</tr>
</tbody>
</table>

## Chapter 1 - Introduction

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audience</td>
<td>5</td>
</tr>
<tr>
<td>ACS Access and Configuration</td>
<td>5</td>
</tr>
<tr>
<td>Product Models and Components</td>
<td>6</td>
</tr>
<tr>
<td>ACS Setup Diagram</td>
<td>8</td>
</tr>
</tbody>
</table>

## Chapter 2 - Installing the ACS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Package Contents</td>
<td>9</td>
</tr>
<tr>
<td>Rack Mounting the ACS</td>
<td>12</td>
</tr>
<tr>
<td>System Requirements</td>
<td>13</td>
</tr>
<tr>
<td>Installation and Configuration Process</td>
<td>15</td>
</tr>
<tr>
<td>Task 1: Install ACS and connect to the network</td>
<td>15</td>
</tr>
<tr>
<td>Task 2: Configure network settings</td>
<td>16</td>
</tr>
<tr>
<td>Task 3: Configure via Web Wizard</td>
<td>18</td>
</tr>
<tr>
<td>Task 4: Test Configuration</td>
<td>18</td>
</tr>
<tr>
<td>Task 5: Configure the web interface in Expert Mode</td>
<td>18</td>
</tr>
<tr>
<td>Task 6: Save Changes</td>
<td>18</td>
</tr>
</tbody>
</table>

## Chapter 3 - Using the Web Interface

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Using the Web Interface</td>
<td>19</td>
</tr>
<tr>
<td>Using the Command Line Interface (CLI)</td>
<td>21</td>
</tr>
<tr>
<td>Logging onto the Terminal</td>
<td>22</td>
</tr>
<tr>
<td>ts_menu Access</td>
<td>23</td>
</tr>
<tr>
<td>Power Management</td>
<td>25</td>
</tr>
<tr>
<td>Security</td>
<td>26</td>
</tr>
</tbody>
</table>
# Chapter 4 - Configuring the Web Interface

<table>
<thead>
<tr>
<th>Overview</th>
<th>27</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logging In</td>
<td>28</td>
</tr>
<tr>
<td>ACS Web Interface: GUI Elements</td>
<td>30</td>
</tr>
<tr>
<td>Wizard Mode</td>
<td>30</td>
</tr>
<tr>
<td>Expert Mode</td>
<td>31</td>
</tr>
<tr>
<td>Button Functions</td>
<td>32</td>
</tr>
<tr>
<td>Saving Your Configuration</td>
<td>32</td>
</tr>
<tr>
<td>Configuring in Wizard Mode</td>
<td>34</td>
</tr>
<tr>
<td>Step 1: Network Settings</td>
<td>34</td>
</tr>
<tr>
<td>Step 2: Port Profile</td>
<td>36</td>
</tr>
<tr>
<td>Step 3: Access</td>
<td>38</td>
</tr>
<tr>
<td>Step 4: Data Buffering</td>
<td>42</td>
</tr>
<tr>
<td>Step 5: System Log</td>
<td>44</td>
</tr>
<tr>
<td>Configuring in Expert Mode</td>
<td>45</td>
</tr>
<tr>
<td>Expert Mode Menu</td>
<td>45</td>
</tr>
<tr>
<td>Applications &gt; Connect</td>
<td>48</td>
</tr>
<tr>
<td>Applications &gt; Power Management</td>
<td>49</td>
</tr>
<tr>
<td>Applications &gt; Terminal Profile Menu</td>
<td>58</td>
</tr>
<tr>
<td>Network &gt; Host Settings</td>
<td>60</td>
</tr>
<tr>
<td>Network &gt; Syslog</td>
<td>62</td>
</tr>
<tr>
<td>Network &gt; PCMCIA Management</td>
<td>63</td>
</tr>
<tr>
<td>What is VPN</td>
<td>70</td>
</tr>
<tr>
<td>Network &gt; VPN Connections</td>
<td>72</td>
</tr>
<tr>
<td>SNMP Daemon Settings</td>
<td>74</td>
</tr>
<tr>
<td>Services</td>
<td>79</td>
</tr>
<tr>
<td>Firewall Configuration</td>
<td>80</td>
</tr>
<tr>
<td>Network &gt; Firewall Configuration</td>
<td>81</td>
</tr>
<tr>
<td>Network &gt; Host Table</td>
<td>88</td>
</tr>
<tr>
<td>Network &gt; Static Routes</td>
<td>89</td>
</tr>
<tr>
<td>Security</td>
<td>91</td>
</tr>
<tr>
<td>Users and Groups</td>
<td>91</td>
</tr>
<tr>
<td>Active Ports Sessions</td>
<td>94</td>
</tr>
<tr>
<td>Ports</td>
<td>95</td>
</tr>
<tr>
<td>Ports &gt; Physical Ports</td>
<td>95</td>
</tr>
<tr>
<td>Ports &gt; Virtual Ports</td>
<td>109</td>
</tr>
<tr>
<td>Ports &gt; Ports Status</td>
<td>111</td>
</tr>
<tr>
<td>Administration</td>
<td>113</td>
</tr>
</tbody>
</table>
WELCOME to the AlterPath Console Server User Guide! This manual is designed to guide you in installing and configuring the AlterPath Console Server through the ACS web user interface, as well as 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 Console Server, using the web application interface.

While users may use any available method to configure the ACS, the ACS web interface 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, Wizard, or Command Line Interface (CLI), or read about other advanced features of the ACS, please refer to the ACS Reference 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: Using the Web Interface  
Explains how to access devices and operate the web interface. This chapter is designed for the ACS regular user.
4: Configuring the Web Interface

Presents the procedures for configuring the ACS, using the web interface. All the procedures follow the menu structure of the entire web interface in Wizard Mode and Expert Mode.

Appendix A

Summarizes the **Hardware Specifications** of the AlterPath Console Server, and lists the PCMCIA cards that the ACS supports.

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 key words or subjects.

**Typographical Conventions**

- **Form/Window labels**: Words that appear on forms, windows, or any part of the user interface are typed in **boldface**.
  
  *Examples:*
  
  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 underlined words are hypertext links.

- **Important words**: For emphasis, important words are **italicized**.

- **Menu selections**: The order in which you select a menu is indicated by the “greater than” symbol (>).

  *Example: Network > Access Method.*

- **Screen words**: Words that appear as part of the graphical user interface are typed in **boldface**.

  *Examples: 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.

*Example:*

```
[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.

*Examples:*

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 **courier**.

*Example:*

```
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.

*Example:*

```
Security > Users and Groups > Add
```

### Naming Conventions

<table>
<thead>
<tr>
<th>Short Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ACS</strong></td>
<td>Short name for the Cyclades AlterPath Console Server.</td>
</tr>
<tr>
<td><strong>Dialog box</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Form</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>
Before You Begin

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 *select* is the same as to *click your mouse*.

Document Symbols

This manual uses graphical symbols that are associated with specific types of note or information to indicate the following:

- Reference to another page or document.
- Note
- Important
- Danger or Warning

Cross References

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

- ACS Reference 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
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.

Audience

This manual is designed primarily for system administrators and regular users who configure and operate the ACS using the web browser, and who are fairly new to Linux.

For all configurations that involve using the VI text editor or command line interface (CLI), please refer to the ACS Reference Guide.

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.

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 Installation
- Installation and Configuration Process

For configuration procedures using vi or CLI, refer to the ACS Reference Guide.

Package Contents

There are six models of the AlterPath Console Server based on the number of serial ports:
- ACS48
- ACS32
- ACS16
- ACS8
- ACS4
- ACS1

All models come with either a single (A/C or VDC) or double (A/C or -48 VDC) power supply.
Package Contents: ACS4 through ACS48

Typically, the product package for ACS4 through ACS48 contains the following:

- ACS Box
- Power Cable(s)
- ADB0017 - DB25F Console Adapter
- ADB0025 - DB25M Console Adapter
- ADB0036 - DB9F Console Adapter
- ADB0039 - Sun/Netra Adapter
- CAB0018 - RJ45 CAT-5 Cable
- CAB0025 - DB25M Straight-Through Cable
- CON0071 - DB25F Loopback Connector
- Rack-Mounting Kit
- ACS User Manual and ACS QuickStart Guide
- ACS Reference Manual CD
**Package Contents: ACS1**

The ACS1 Package contains the following:

- ACS1 Box
- Power Cable
- Power Supply +5V / 2.5A
- CAB0042 - DB25F / DB9F Cross Cable
- CAB0018 - RJ45 / RJ45 CAT5 Cable
- CON0071 - DB25F Loopback Connector
- ADB0036 - RJ45 to DB9F Adapter
- CON0093 - DB9F to DB25M Connector
- ACS User Manual and ACS QuickStart Guide
- ACS Reference Manual CD
Although the ACS unit in the figures are shown with a dual power supply (A/C or -48VDC), some models may have a single power supply. The single power units will have just one power cable. (ACS48 supports -48VDC.)

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 corners of the box using a screw driver and the screws and bolts provided with the mounting kit.

2. Mount the ACS box in a secure position. Refer to Appendix B: Safety Guidelines section of this manual to ensure safety.

**Important!** Install your AlterPath Console Server near the power managed equipment and in an easily accessible location.

**Important!** Install the AlterPath Console Server in a location 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 hardware connectivity required for each configuration method:

<table>
<thead>
<tr>
<th>Hardware Connectivity</th>
<th>Configuration Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Workstation, Hub Ethernet Cables.</td>
<td>Web browser, vi, Wizard, or CLI</td>
</tr>
<tr>
<td>Console, Console Cable (constructed from RJ45 straight-through cable + adapter</td>
<td>vi, Wizard, or CLI.</td>
</tr>
<tr>
<td>Workstation, Hub Ethernet Cables.</td>
<td></td>
</tr>
</tbody>
</table>

This manual is designed primarily for web browser users. If you will use vi, the wizard (CLI version) or CLI, refer to the ACS Reference Guide.

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

<table>
<thead>
<tr>
<th>Access/Software</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Root Access</td>
<td>You will need Root Access on your local UNIX machine in order to use the serial port.</td>
</tr>
<tr>
<td>HyperTerminal, Kermit, or Minicom</td>
<td>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.</td>
</tr>
<tr>
<td>IP Address of: PC or terminal, AlterPath Console Server, NameServer, and Gateway</td>
<td>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.</td>
</tr>
<tr>
<td>Network Access</td>
<td>You must have a NIC card installed in your PC to provide an Ethernet port, and have network access.</td>
</tr>
<tr>
<td>Java 2 JRE</td>
<td>You must have Java 2 Runtime Environment (JRE) version 1.4.2 (which can be found at <a href="http://java.sun.com/">http://java.sun.com/</a>) installed on your PC with your browser acknowledged to use it.</td>
</tr>
</tbody>
</table>

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:

- Task 1: Install ACS and connect to the network.
- Task 2: Configure the network settings (using the console port).
- Task 3: Configure ACS by using the web in Wizard Mode.
- Task 4: Test Configuration.
- Task 5: Customize configuration by using the web in Expert Mode.
- Task 6: Save Changes.

You can configure ACS using the command line interface alone. See the ACS Reference Guide to configure ACS in CLI.

Task 1: Install ACS and connect to the network

1. Plug the power cable into the ACS.
   (When using an external power source. Optional.) 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.

   **DANGER!** 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.

   **IMPORTANT!** The AlterPath Console Server must be plugged into a receptacle protected by an appropriate, listed circuit breaker.

2. 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.
2: Installing the ACS

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.

3. Connect to the Network.
   Connect the ACS network port to the Ethernet hub switch.

**Task 2: Configure network settings**

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 via the network using the default network settings.

**Initial Configuration Using the ACS 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.hilgreve.com/htpe/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 values:
   - 9600 bps
   - 8 data bits
   - No parity
   - 1 stop bit
   - No flow control
4. Power on the ACS.
   Click **OK** on the Properties window.
   You will see the ACS booting on your screen. After it finishes booting,
you will see a login prompt.

5. Connect COM Port to the ACS Console.
   Login as **root**, and enter the default password, **tslinux**.

6. Type in: **wiz**
   As shown in the sample screen below, the system brings up the
   configuration wizard banner and begins running the wizard. Follow the
   system prompts to either accept the default values or enter them manually.

```
Login as: root
Password:
[root@CAS root]# wiz
******************************************************************************
********** CONFIGURATION WIZARD **********
******************************************************************************

INSTRUCTIONS for using the Wizard:
You can:
  1| Enter the appropriate information for your system
     and press ENTER or
  2| Press ENTER if you are satisfied with the value
     within the brackets [ ] and want to go on to the
     next parameter or
  3| Press ESC if you want to exit.

NOTE: For some parameters, if there is nothing within
the brackets, it will continue to ask for a value.
In that case, you must enter a valid value or # if you
do not wish to configure the value.

Press ENTER to continue...
******************************************************************************
```

*For the procedure on how to configure the ACS from wiz to support
Kerberos tickets, refer to the ACS Reference Guide.*

7. Proceed to Task 3.
After the initial configuration, you can configure the network further by using any of the following methods:

- Web Interface
- Command Line Interface via SSH
- AlterPath Manager, if installed in your network

To use the ACS web management interface, ask your System Administrator for the IP address. By default, ACS uses the IP address provided by the DHCP server. If your network doesn’t have DHCP, then ACS will default to 192.168.160.10. Configure your ACS to connect to this address and run the web interface.

**Task 3: Configure via Web Wizard**

Proceed to Chapter 4: Configuring the Web Interface, and complete the procedure for configuring ACS in Wizard Mode.

**Task 4: Test Configuration**

Log in as a regular user and connect to a port.
Check the other features (e.g., Data Buffering, Management, etc.) as discussed in Chapter 3: Using the ACS.

To create new users, see Wizard Mode Step 3: Access (page 4-10) of Chapter 4: Configuring the Web Interface.

**Task 5: Configure the web interface in Expert Mode**

Return to Chapter 4: Configuring the Web Interface and continue with configuration using the Expert Mode.

**Task 6: Save Changes**

Click on the Apply Changes button located on the bottom of the ACS Web Configuration screen when done to save your configuration to Flash.
Chapter 3
Using the Web Interface

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 Interface
- Using the Command Line Interface
- Using Telnet
- Using the TS Menu
- Power Management

Using the Web Interface

Refer to Appendix B for a description of the web requirements for connecting to a serial port.

To use the web interface 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.
3: Using the Web Interface

The system brings up the ACS Web Application Login Window:

3. To log in, type in your username and password as provided to you by your system administrator.
4. From the top menu bar, select **Applications**; from the left menu panel, select **Connect**.

The system brings up the Port Selection form:
5. To connect to a port (by default, the radio button is already selected for connecting to a port), select from the drop down menu the port 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 Box, 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 a chosen server.

![Sample Screen](image)

**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 **SndBreak** button.

The upper right hand corner of the browser (Java window) shows two icons: Refresh and Disconnect.

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

**Logging onto 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 AlterPath ACS (Ethernet's interface) as configured by the user or as learned from DHCP.

<TCP port number> is the number associated to the serial port. The factory 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's "\[Ctrl-\]").

**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 and ssh2. The AlterPath Console Server offers both.
To open a 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.
- `<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
   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 (Application > Power Management > Outlets Manager or View IPDUs Info) allows you to manage the power outlets on the Cyclades 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 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 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: Configuring the Web Interface.
3: Using the Web Interface

Security

The Security form allows you to change your password.

1. From the menu panel, select **Security**.
   The system brings up the **Security** form.

2. From the **Security** form enter your current password and new password (twice).
3. Select **OK** when done.
4. Log out and log in using your new password to verify your password change.
This chapter presents the procedures for configuring ACS using the web interface. It is organized as follows:

Overview
Logging In

ACS Web Interface: GUI Elements

Configuring in Wizard Mode
  Step 1: Network Settings
  Step 2: Port Profile
  Step 3: Access
  Step 4: Data Buffering
  Step 5: 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 interface and its users. For information on how to configure ACS using vi or Command Line Interface (CLI), please consult the ACS Reference Guide.

The ACS web configuration interface provides two modes of operation: Wizard and Expert. The organization of the chapter follows, in sequential order, the two modes and the menu selections available from each mode.

If you are a regular user, refer to Chapter 3: Using the Web Interface.
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.

   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.

The system brings up the AlterPath ACS Login page:

2. Log in as root and type in the Web root password configured by the Web server.

   The system brings up the ACS Web management page.
If another administrator is using the system, the following message appears:

![Message](image)

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

**IMPORTANT:** Take note of this login procedure. All subsequent online procedures in this chapter assume that you are already logged in.
ACS Web Interface: GUI Elements

The ACS web interface operates on two modes:
- Wizard
- Expert

**Wizard Mode**

The wizard is designed to simplify configuration by providing users the default parameter values. The system will prompt you for the necessary fields, give instructions during the process and, in some cases, populate the fields automatically.

Designed for the novice, the wizard mode allows you to perform the basic configuration necessary to set up ACS and users in the quickest possible way. When you log in to ACS, the system brings up by default the Expert Mode screen. To change to the Wizard Mode, click on the button located in the left bottom corner of the screen labeled **Wizard**.
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 the ACS. You can also change to this mode by clicking the Expert button at the bottom of the menu panel switches the web interface from Wizard to Expert Mode. Shown below is a typical ACS screen in Expert Mode. A main difference between the two modes is the addition of a top menu bar in the Expert Mode to support a wider array of menu choices.

The top menu bar is the primary menu; the left menu panel is the secondary menu. Based on what you select from the top menu bar, the left menu selections will change accordingly..
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 Configuration window provide you the following functions for operating the interface.

<table>
<thead>
<tr>
<th>Button Name</th>
<th>Use this button to:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wizard / Expert</td>
<td>Wizard / Expert Switch the ACS Web Configuration Screen to either Expert or Wizard Mode. The Expert Mode is the default mode; in this mode, the Wizard button is visible and vice versa.</td>
</tr>
<tr>
<td>Help?</td>
<td>Invoke the online help sub window which provides help information relating to the current form.</td>
</tr>
<tr>
<td>Back</td>
<td>Traverse to the previous form (i.e., the form preceding the current form as it appears in the menu).</td>
</tr>
<tr>
<td>Try Changes</td>
<td>Test or run the system based on the settings from the current form without having to save the configuration.</td>
</tr>
<tr>
<td>Cancel Changes</td>
<td>Cancel your changes or reverts back to the original configuration values.</td>
</tr>
<tr>
<td>Apply Changes</td>
<td>Save your changes to the ACS Flash card.</td>
</tr>
<tr>
<td>Next</td>
<td>Traverse to the next form (i.e., the form succeeding the current form as it appears in the menu).</td>
</tr>
</tbody>
</table>

**Saving Your Configuration**

The Unsaved Changes indicator on the lower right hand corner of the ACS web configuration window serves to remind you that you have made a configuration entry or change which has not been saved.
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 in Wizard Mode

As shown in the menu, the Wizard Mode configuration is composed of five steps:

Step 1: Network Settings
Step 2: Port Profile
Step 3: Access
Step 4: Data Buffering
Step 5: System Log

**Step 1: Network Settings**

To configure the network settings for the ACS, follow the following steps:

1. From the main menu of the web interface, select **Step 1: Network Settings**.

The system brings up the DHCP page (shown below). By default, the DHCP checkbox is check marked, which means that the system is already configured to use the DHCP server.
2. If you are using DHCP, proceed to **Step 2: 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:

   ![Network Settings Screen Capture]

   3. Type in the network information in the corresponding entry fields, and then select **Apply Changes**.

   If the meaning of a field is unclear, select the **Help** button for a definition of the field.

   4. Select the **Next** button OR proceed to **Step 2: Port Profile** section.
Step 2: 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.

In Wizard mode the system assumes that all devices will be connected at the same parameter values.

*If you need to configure different values to specific devices, then you must click on the Expert mode button and select Ports > Physical Ports to enter these values.*

1. From the main menu of the web interface, select **Step 2: Network Settings**.

   The system displays the Port Profile form:

   ![Port Profile Form](image)

2. From the Port Profile form, complete the necessary fields.
If you require port authentication, then you must add users through Wizard *Step 3: Access.*

To configure other authentication methods (e.g., LDAP, RADIUS, TACACS), select the Expert button to switch to Expert Mode and select: Security > Authentication.

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

4. Select the **Next** button or proceed to the next section, **Step 3: Access.**
Step 3: Access

The Wizard configuration of the Access form enables you to configure the general access rights of users and groups to the ACS or systems which ACS controls.

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

1. If you haven’t opened the Access Form, from the menu panel, select Step 3: Access.
   The system brings up the Access form:

   ![Access Form]

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.
Changing a User Password

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 select the Change Password button.

The system brings up the Change User Password dialog box:

![Change User Password dialog box]

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

1. If you haven’t opened the Access form, select **Step 3: 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:

   ![Add User Dialog Box](image)

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

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name</td>
<td>Name of the ACS user.</td>
</tr>
<tr>
<td>Password</td>
<td>Password to be used by the user to access ACS.</td>
</tr>
<tr>
<td>Repeat Password</td>
<td>Re-type the password.</td>
</tr>
<tr>
<td>Group</td>
<td>Select the user group to which the user belongs.</td>
</tr>
<tr>
<td></td>
<td>There are two default groups with the following</td>
</tr>
<tr>
<td></td>
<td>associated access rights:</td>
</tr>
<tr>
<td></td>
<td>Admin (Read/Write)</td>
</tr>
<tr>
<td></td>
<td>Regular User (Read Only)</td>
</tr>
</tbody>
</table>

---

*AlterPath Console Server User Manual*
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.

### Deleting 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.

<table>
<thead>
<tr>
<th><strong>Field Name</strong></th>
<th><strong>Definition</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>[dropdown list]</td>
<td>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).</td>
</tr>
<tr>
<td>Shell</td>
<td>Text string you wish to use as part of the shell prompt for the current user.</td>
</tr>
<tr>
<td>Comments</td>
<td>Comments about the current user.</td>
</tr>
</tbody>
</table>
**Step 4: 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 5: System Log**. Do not click on the **Enable Data Buffering** checkbox.

1. From the menu panel, select **Step 4: Data Buffering**.
   The system brings up the Data Buffering form:

   ![Data Buffering Form](image)

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>
<thead>
<tr>
<th>Field Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination</td>
<td>Destination of the buffer files: Local (i.e., Ramdisk) or Remote.</td>
</tr>
<tr>
<td>Mode</td>
<td>If you selected Local destination, choose the file sort mode. Select Linear for sequential files, Circular for non-sequential files.</td>
</tr>
<tr>
<td>File Size (Bytes)</td>
<td>If you selected Local destination, the value for this field cannot be zero.</td>
</tr>
<tr>
<td>Record the time stamp...</td>
<td>Commands the system to include a time stamp in the buffer.</td>
</tr>
<tr>
<td>Data Buffering file</td>
<td>Name of the buffer file.</td>
</tr>
<tr>
<td>Show Menu</td>
<td>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.</td>
</tr>
</tbody>
</table>

4. 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](image)

5. 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**).

**Step 5: 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.

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

1. From the menu panel, select **System Log**.
   
The system brings up the System Log form:

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

This section presents the procedures for configuring the ACS web interface in Expert Mode. This mode is designed for the advanced user 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
- Network
- Security
- Ports
- Administration

Expert Mode Menu

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

### Applications

<table>
<thead>
<tr>
<th>Menu Selection</th>
<th>Use this menu to:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connect</td>
<td>Select and connect to a port.</td>
</tr>
<tr>
<td>Power Management</td>
<td>View and edit IPDU settings. This menu comprises five tabbed forms: Outlets Manager, View IPDUs Info, Users Manager, Configuration, and Software Upgrade.</td>
</tr>
</tbody>
</table>
Most of the fields for each form are defined in the procedure. For a more detailed definition of these field names or terms, however, refer to the Glossary of this manual.

### Network

<table>
<thead>
<tr>
<th>Menu Selection</th>
<th>Use this menu to:</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Terminal Profile Menu</strong></td>
<td>Create command menu for a terminal (i.e., CLI or VI).</td>
</tr>
<tr>
<td><strong>Host Settings</strong></td>
<td>Configure host connections, including: Ethernet Port connections, DNS Service, and Name Service Access.</td>
</tr>
<tr>
<td><strong>Syslog</strong></td>
<td>Define the Syslog Servers to enable system logging.</td>
</tr>
<tr>
<td><strong>PCMCIA Management</strong></td>
<td>Enable the insertion or ejection of PCMCIA cards; configure the type of access and connection (e.g., Modem, ISDN, Ethernet) to ACS.</td>
</tr>
<tr>
<td><strong>VPN Connections</strong></td>
<td>Configure IPsec tunnels to establish a secure connection between ACS and a security gateway machine.</td>
</tr>
<tr>
<td><strong>SNMP Daemon Settings</strong></td>
<td>Configure the SNMP server to manage complex networks.</td>
</tr>
<tr>
<td><strong>Services</strong></td>
<td>Define or activate the method of access (i.e., Telnet, SSH, SNMP, Client, or NTP).</td>
</tr>
<tr>
<td><strong>Firewall Configuration</strong></td>
<td>Configure static IP tables.</td>
</tr>
<tr>
<td><strong>Host Table</strong></td>
<td>View table of hosts; create, edit, and delete hosts.</td>
</tr>
<tr>
<td><strong>Static Routes</strong></td>
<td>View, create and delete routes from the table.</td>
</tr>
</tbody>
</table>

### Security

<table>
<thead>
<tr>
<th>Menu Selection</th>
<th>Use this menu to:</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Users and Groups</strong></td>
<td>Create/edit users and groups, establish/change their passwords, access rights and privileges.</td>
</tr>
<tr>
<td><strong>Active Port Sessions</strong></td>
<td>View the status of all active port sessions.</td>
</tr>
</tbody>
</table>
## Ports

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

## Administration

<table>
<thead>
<tr>
<th>Menu Selection</th>
<th>Use this menu to:</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Information</td>
<td>View summary information about the system (e.g., Kernel, CPU, memory, etc.).</td>
</tr>
<tr>
<td>Notifications</td>
<td>Configure the system to deliver alarm notification by email, pager, or snmp trap; define alarm triggers; set data buffering to send notification.</td>
</tr>
<tr>
<td>Time/Date</td>
<td>Set the unit’s date and time.</td>
</tr>
<tr>
<td>Boot Configuration</td>
<td>Defines the settings for loading the operating system in the event that the ACS fails to boot successfully.</td>
</tr>
<tr>
<td>Backup Configuration</td>
<td>Use a FTP server to save and retrieve your ACS configuration; use a storage device to store your configuration.</td>
</tr>
<tr>
<td>Upgrade Firmware</td>
<td>Upload/upgrade new firmware.</td>
</tr>
<tr>
<td>Reboot</td>
<td>Reboot the ACS system.</td>
</tr>
</tbody>
</table>
4: Configuring the Web Interface

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 what 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:

2. To connect to a port (by default, the radio button is already selected for connecting to a port), select from the drop down menu the port 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 Box, 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.
Applications > 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>
<thead>
<tr>
<th>Form Title</th>
<th>Use this form to:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Outlets Manager</td>
<td>Switch on/off and lock/unlock outlets.</td>
</tr>
<tr>
<td>View IPDUs Info</td>
<td>View IPDU information by ports and slaves. The information form provides real-time, global, current monitoring of all connected devices.</td>
</tr>
<tr>
<td>Users Manager</td>
<td>Add or delete users assigned to specific outlets.</td>
</tr>
<tr>
<td>Configuration</td>
<td>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.</td>
</tr>
<tr>
<td>Software Upgrade</td>
<td>Upgrade power management software.</td>
</tr>
</tbody>
</table>

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

   ![Outlet Manager 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.

To save your changes, click on the **Save Outlets State** button located in the form.

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:

   ![Edit Outlet dialog box](image)

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.
Applications > Power Management > 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.

   The system brings up the IPDUs Info form:

   ![IPDUs Info Form]

   **Serial Port 4: General Information**
   - Name: PowerMgm-4
   - Syslog: ON
   - Number of Outlets: 8
   - Number of Units: 1
   - Buzzer: OFF
   - Over Current Protection: OFF

   **Master Unit Information**
   - Model: PMB1S5A
   - Software Version: 1.2.0
   - Alarm Threshold: 15.0A
   - Current: 0.0A
   - Temperature: 0.0A
   - Maximum Detected Current: 0.4A
   - Maximum Detected Temperature: OFF

2. To delete the stored values for the maximum detected current, select the Clear Max Detected Current button.

3. To delete the stored values for the maximum detected temperature, select the Clear Max Detected Temperature button.
Applications > Power Management > 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:

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:
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.

   *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.

**Deleting 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.
Applications > Power Management > 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:

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.
Applications > Power Management > 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:

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 detected 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:

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.
4: Configuring the Web Interface

**Applications > 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:

   ![Terminal Profile Menu Form](image)

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.
3. Type in the menu title and/or action to the corresponding entry fields and then select **Apply**.
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 > Host Settings

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

1. Select **Network** from the top menu bar, and then select **Host Settings** from the left menu panel.

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

   By default, the DHCP field is check marked. If you wish to disable DHCP and enter the host settings manually, click the checkbox to remove the check mark.

   The system should add the following fields to your form:
2. From the Host Settings form, complete or edit the following fields, as necessary:

<table>
<thead>
<tr>
<th>Filed Name</th>
<th>Field Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Name</td>
<td>The fully qualified domain name identifying the specific host computer within the Internet.</td>
</tr>
<tr>
<td>Console Banner</td>
<td>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.</td>
</tr>
<tr>
<td>Ethernet Port</td>
<td></td>
</tr>
<tr>
<td>Primary IP</td>
<td>IP address of the unit.</td>
</tr>
<tr>
<td>Secondary IP</td>
<td>The second IP address of the unit. Configuring the second IP address, the unit will be available for more than one network.</td>
</tr>
<tr>
<td>Network Mask</td>
<td>The 32-bit number used to group IP addresses together or to indicate the range of IP addresses for this IP network/subnet/supernet.</td>
</tr>
<tr>
<td>Secondary Network Mask</td>
<td>Optional.</td>
</tr>
<tr>
<td>MTU</td>
<td>Maximum Transmission Unit used by the TCP protocol.</td>
</tr>
<tr>
<td>DNS Service</td>
<td></td>
</tr>
<tr>
<td>DNS Server</td>
<td>Address of the Domain Name Server.</td>
</tr>
<tr>
<td>Secondary DNS Server</td>
<td>Address of the backup Domain Name Server.</td>
</tr>
<tr>
<td>Domain Name</td>
<td>The name that identifies the domain (e.g., domainname.com).</td>
</tr>
<tr>
<td>Gateway IP</td>
<td>As indicated.</td>
</tr>
</tbody>
</table>

3. Select the Apply Changes button at the bottom of the application window to complete the procedure.
Network > 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.

1. Select Network from the top menu bar, and then select Syslog from the left menu panel.

The system brings up the Syslog form.

2. Complete the form as follows:

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Facility Number</td>
<td>Facility number to identify the location of the Syslog Server.</td>
</tr>
<tr>
<td>New Syslog Server</td>
<td>Name of the Syslog Server that you wish to add.</td>
</tr>
<tr>
<td>Syslog Servers</td>
<td>List of all Syslog Servers connected to ACS.</td>
</tr>
</tbody>
</table>
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
   - OR -
   To delete a Syslog Server, from the **Syslog Servers** list box, select the server you wish to delete, and then select **Delete**.
4. Select **Apply Changes** to save your changes to Flash.

**Network > 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. Cyclades ACS supports several PCMCIA cards including modem, ISDN, wireless and wired NICs, Compact Flash and IDE drives for data buffer storage.

*For a list of all ACS-supported PCMCIA Cards, refer to Appendix A: Hardware Specifications.*

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.

1. Select **Network** from the top menu bar, and then select **PCMCIA Management** from the left menu panel.

The system brings up the 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.
   The system brings up the PCMCIA Configuration dialog box:

![PCMCIA Configuration Dialog Box](image)

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

![Modem Configuration Dialog Box]

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>[PCMCIA Card]</td>
<td>Pull-down box to select the type of PCMCIA card that you are using.</td>
</tr>
<tr>
<td>PPP</td>
<td>Check box to enable point-to-point protocol.</td>
</tr>
<tr>
<td>Local IP</td>
<td>The local IP address of the PCMCIA card.</td>
</tr>
<tr>
<td>Remote IP</td>
<td>The remote IP address of the PCMCIA card.</td>
</tr>
<tr>
<td>Call Back</td>
<td>Check box to enable the callback security feature.</td>
</tr>
<tr>
<td>Phone Number</td>
<td>The phone number that the ACS uses to call back.</td>
</tr>
</tbody>
</table>
Access Method: ISDN

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

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>[PCMCIA Card]</td>
<td>Select ISDN from the pull-down box.</td>
</tr>
<tr>
<td>PPP</td>
<td>Check box to enable point-to-point protocol.</td>
</tr>
<tr>
<td>Local IP</td>
<td>The local IP address of the PCMCIA card.</td>
</tr>
<tr>
<td>Remote IP</td>
<td>The remote IP address of the PCMCIA card.</td>
</tr>
<tr>
<td>Call Back</td>
<td>Check box to enable the callback security feature.</td>
</tr>
<tr>
<td>Phone Number</td>
<td>The phone number that the ACS uses to call back.</td>
</tr>
</tbody>
</table>
Access Method: GSM

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

![Image of GSM interface]

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>[PCMCIA Card]</td>
<td>Select GSM from the pull-down box.</td>
</tr>
<tr>
<td>Local IP</td>
<td>The local IP address of the PCMCIA card.</td>
</tr>
<tr>
<td>Remote IP</td>
<td>The remote IP address of the PCMCIA card.</td>
</tr>
<tr>
<td>Pin Number</td>
<td>The personal identification number associated with the GSM.</td>
</tr>
<tr>
<td>Call Back</td>
<td>Check box to enable the callback security feature.</td>
</tr>
</tbody>
</table>
4: Configuring the Web Interface

**Access Method: Ethernet**

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

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>[PCMCIA Card]</td>
<td>Select <em>Ethernet</em> from the Pull-down box.</td>
</tr>
<tr>
<td>IP Address</td>
<td>The local IP address of the Ethernet.</td>
</tr>
<tr>
<td>Network Address</td>
<td>The network address of the Ethernet.</td>
</tr>
</tbody>
</table>

**Access Method: Compact Flash**

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

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>[PCMCIA Card]</td>
<td>Select <em>Compact Flash</em> from the Pull-down box.</td>
</tr>
<tr>
<td>Enable</td>
<td>Check box to enable the compact flash.</td>
</tr>
<tr>
<td>Use for Data Buffering</td>
<td>Check box to use the compact flash for data buffering.</td>
</tr>
</tbody>
</table>
4: Configuring the Web Interface

Access Method > Wireless LAN

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

![Image of Wireless LAN settings]

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>[Unlabeled]</td>
<td>Pull-down box to select the type of PCMCIA card that you are using.</td>
</tr>
<tr>
<td>PPP</td>
<td>Check box to enable point-to-point protocol.</td>
</tr>
<tr>
<td>Local IP</td>
<td>The local IP address of the PCMCIA card.</td>
</tr>
<tr>
<td>Remote IP</td>
<td>The remote IP address of the PCMCIA card.</td>
</tr>
<tr>
<td>Call Back</td>
<td>Check box to enable the callback security feature.</td>
</tr>
<tr>
<td>Phone Number</td>
<td>The phone number that the ACS uses to call back.</td>
</tr>
</tbody>
</table>
What is VPN

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

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 rightnexthop (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 AlterPath Console Server 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.
Network > 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.

1. Select Network from the top menu bar, and then select VPN Connections from the left menu panel.
   The system brings up the 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 -
   To add a VPN connection, select the Add button.
The system brings up the **New/Modify VPN Connection** dialog box:

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>
<thead>
<tr>
<th><strong>Field Name</strong></th>
<th><strong>Definition</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Connection Name</strong></td>
<td>Name of the VPN connection.</td>
</tr>
<tr>
<td><strong>Authentication Protocol</strong></td>
<td>Authentication protocol used to establish a VPN connection.</td>
</tr>
<tr>
<td><strong>Authentication Method</strong></td>
<td>Authentication method used to establish a VPN connection.</td>
</tr>
<tr>
<td><strong>Remote (“Right”)</strong></td>
<td></td>
</tr>
<tr>
<td><strong>ID</strong></td>
<td>Identification name.</td>
</tr>
<tr>
<td><strong>IP Address</strong></td>
<td>Remote IP address.</td>
</tr>
<tr>
<td><strong>NextHop</strong></td>
<td>The router to which the Console Server sends packets in order to deliver them to the left.</td>
</tr>
<tr>
<td><strong>Subnet Mask</strong></td>
<td>As indicated.</td>
</tr>
</tbody>
</table>
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 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

<table>
<thead>
<tr>
<th><strong>Field Name</strong></th>
<th><strong>Definition</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>RSA Key</td>
<td>You may use the copy and paste feature of your browser to enter the RSA key.</td>
</tr>
<tr>
<td><strong>Local (“Left”)</strong></td>
<td></td>
</tr>
<tr>
<td>ID</td>
<td>Identification name.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Local IP address.</td>
</tr>
<tr>
<td>NextHop</td>
<td>The router to which the Console Server sends packets in order to deliver them to the right.</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>As indicated.</td>
</tr>
<tr>
<td>RSA Key</td>
<td>You may use the copy and paste feature of your browser to enter the RSA key.</td>
</tr>
<tr>
<td>Boot Action</td>
<td>Boot action with regards to generating an RSA key pair upon system boot.</td>
</tr>
<tr>
<td>Pre-Shared Secret</td>
<td>The pre-shared password between left and right users.</td>
</tr>
</tbody>
</table>
configurations. SNMPv1/v2 requires community, source, object ID and the type of community (read-write, read-only). V3 requires user name.

**Important! Check the SNMP configuration before gathering information about 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. From the top menu bar, select **Networks**; from the left menu panel, select **SNMP Daemon Settings**.

   The system invokes the SNMP Daemon Settings form:

   ![SNMP Daemon Settings Form]

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

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Community</td>
<td>The community name acts as a password to authenticate messages sent between an SNMP client and a router containing an SNMP server. The community name is sent in every packet between the client and the server.</td>
</tr>
</tbody>
</table>
If you are using SNMPv3, skip steps 2 and 3; proceed to step 4.

3. To Add an SNMP agent using SNMPv1/SNMP2 Configuration, select the **Add** button located at the bottom of this view table.
   - OR -
   To edit an SNMP agent, select the **Edit** button.
   The system invokes the **New/Modify v1 v2 Configuration** dialog box:

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>SysContact</td>
<td>The email of the person to contact regarding the host on which the agent is running (e.g., <a href="mailto:me@mymachine.mydomain">me@mymachine.mydomain</a>)</td>
</tr>
<tr>
<td>SysLocation</td>
<td>The physical location of the system (e.g., mydomain).</td>
</tr>
</tbody>
</table>

4. Complete the dialog box as follows:

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Community</td>
<td>The password used to authenticate messages sent between the SNMP client and the router containing the SNMP server.</td>
</tr>
<tr>
<td>Source</td>
<td>The IP addresses or the range of source IP address.</td>
</tr>
<tr>
<td>OID</td>
<td>Object Identifier.</td>
</tr>
</tbody>
</table>
5. If you are adding or editing an SNMP agent using SNMPv3, scroll down to the lower half of the SNMP Configuration form:

6. 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.
4: Configuring the Web Interface

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

7. Complete the form and when done, select the **OK** button from the dialog box.
8. Verify your entry or modification from the respective tables of the SNMP Configuration form.
9. Select the **Apply Changes** button to complete the procedure.
Services

The **Services** form is used to enable or disable the daemons to use to allow different incoming connections.

1. From the top menu, select **Network**; from the left menu panel, select **Services**.
   The system invokes the Services form.

2. From the Services form, select the service(s) you wish to use.
3. Select the **Apply Changes** button to save your configuration.
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:

- 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.

**Network > Firewall Configuration**

1. Select **Network** from the top menu bar, and then select **Firewall Configuration** from the left menu panel.

   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.
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.
   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:

   ![Edit Rules for Chain 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.
The system brings up the **Edit Rule** dialog box:

![Edit Rule dialog box](image)

3. Complete the necessary fields as follows:

<table>
<thead>
<tr>
<th><strong>Field Name</strong></th>
<th><strong>Definition</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Target</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Source IP</strong></td>
<td>The source IP address.</td>
</tr>
<tr>
<td><strong>Mask</strong></td>
<td>Source network mask. Required when a network should be included in the rule.</td>
</tr>
<tr>
<td><strong>Inverted</strong></td>
<td>Select box to invert the target action (<em>i.e.</em>, the action assigned to the target will be performed to all source IPs/Masks except to the one just defined).</td>
</tr>
</tbody>
</table>
### Field Name | Definition
--- | ---
**Destination IP** | Destination IP address.
**Mask** | Destination network mask.
**Inverted** | Select box to invert the target action (i.e., 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.e., 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.e., 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.e., IP Tables) can check for:
- All Packets.
- 2nd, 3rd... fragmented packets.
- Non-fragmented and 1st fragmented packets.
**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.
4: Configuring the Web Interface

Additional Fields

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

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Level</td>
<td>The log level classification to be used based on the type of error message (e.g., alert, warning, info, debug, etc.).</td>
</tr>
<tr>
<td>Log Prefix</td>
<td>The prefix that will identify the log.</td>
</tr>
<tr>
<td>TCP Sequence</td>
<td>Check box to include TCP sequence in the log.</td>
</tr>
<tr>
<td>TCP Options</td>
<td>Check box to include TCP options in the log.</td>
</tr>
<tr>
<td>IP Options</td>
<td>Check box to include IP options in the log.</td>
</tr>
</tbody>
</table>

If you selected Reject as the target, the **Reject Options** field appears:

From the scrollable list, select the ICMP message to be associated with the Reject target.

4. Click on the **OK** button when done.

5. 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.
   The system brings up the Edit Rule for Chain dialog box.

3. From the Edit Rule for Chain dialog box, click on the Add button.
   The system brings up the Add Rule dialog box.

4. Complete the Add Rule dialog box. (Refer to the Editing a Rule section for a definition of the input fields, as needed.)

5. 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>
<thead>
<tr>
<th>Field Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reject with</td>
<td>(“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.)</td>
</tr>
<tr>
<td>Choices are:</td>
<td></td>
</tr>
<tr>
<td>icmp-net-unreachable</td>
<td>ICMP network unreachable alias.</td>
</tr>
<tr>
<td>icmp-host-unreachable</td>
<td>ICMP host unreachable alias.</td>
</tr>
<tr>
<td>icmp-port-unreachable</td>
<td>ICMP port unreachable alias.</td>
</tr>
<tr>
<td>icmp-proto-unreachable</td>
<td>ICMP protocol unreachable alias.</td>
</tr>
<tr>
<td>icmp-net-prohibited</td>
<td>ICMP network prohibited alias.</td>
</tr>
<tr>
<td>icmp-host-prohibited</td>
<td>ICMP host prohibited alias.</td>
</tr>
<tr>
<td>echo-reply</td>
<td>Echo reply alias.</td>
</tr>
<tr>
<td>tcp-reset</td>
<td>TCP RST packet alias.</td>
</tr>
</tbody>
</table>

The packets are matched (using tcp flags and appropriate reject type) with the REJECT target.
Network > 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.

1. From the top menu bar, select Network; from the left menu panel, select Host Table.
   The system invokes the Host Tables form:

   ![Host Table Form](image)

   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 -

      To add a host, click the Add button.
      The system brings up the New/Modify Host dialog box:
3. 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.
4. 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.
5. Select the **Apply Changes** button to save your configuration to Flash.

**Network > 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
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.

1. From the top menu bar, select **Network**; from the left menu panel, select
**Static Routes**.

The system brings up the Static Routes table form:

> 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 -

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

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

   ![New/Modify Route dialog box](image)

   Complete the fields as follows:

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

3. 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

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`).

If a step does not apply (e.g., edit, delete), skip to the next step.
4: Configuring the Web Interface

**Adding 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:

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.
   The system brings up the **Add Users and Groups** dialog box:

3. Complete the dialog box shown above, and then select **OK**.
4: Configuring the Web Interface

All users must be assigned to a group.

4. 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.

5. Repeat step 3.

**Deleting 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 -
   To delete a group, select the group name from the Group listbox of the Users and Groups form, and then select the **Delete** button.

**Changing 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.
4: Configuring the Web Interface

**Active Ports Sessions**

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

Open sessions are displayed with their identifications and statistics 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.

1. From the top menu bar, select **Security**; from the left menu panel, select **Active Ports Sessions**.
   
   The system invokes the Active Ports Sessions window:

![Active Ports Sessions Window](image)

The field or column names of the above view table indicate the following:

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>The user who initiated the port session.</td>
</tr>
<tr>
<td>TTY</td>
<td>The name of the serial port.</td>
</tr>
<tr>
<td>From</td>
<td>The network machine to which the port is connected.</td>
</tr>
<tr>
<td>Login</td>
<td>The time of the last login.</td>
</tr>
<tr>
<td>Idle</td>
<td>The time when the port became inactive.</td>
</tr>
</tbody>
</table>
Ports

The Ports section of the ACS configuration in Expert Mode provides two 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 > 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>
<thead>
<tr>
<th>Tab Name</th>
<th>Use this form to:</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td>Define general port settings; Connect to an IPDU port and select the connection type (SSH, Telnet or both).</td>
</tr>
<tr>
<td>Access</td>
<td>Designate users and groups to authenticate, and assign authentication type or server.</td>
</tr>
<tr>
<td>Data Buffering</td>
<td>Define data buffering mode, size, syslog server, etc.</td>
</tr>
<tr>
<td>Multi User</td>
<td>Enable concurrent usage and sniff mode.</td>
</tr>
<tr>
<td>Power Management</td>
<td>Enable Power Management for the selected port(s); assign users and groups to enable them to set the IPDU settings for these port(s).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>JCPU</td>
<td>The duration of time used by all processes attached to the tty. It does not include past background jobs; only currently running background jobs.</td>
</tr>
<tr>
<td>PCPU</td>
<td>The time used by the current process that is named in the <strong>What</strong> column.</td>
</tr>
<tr>
<td>What</td>
<td>The current process attached to the tty.</td>
</tr>
</tbody>
</table>
To configure the ports:

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

The system invokes the Physical Ports Modification 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 -
   To modify all ports, click on the **Modify All Ports** button.

3. Proceed to the next section, **Port Settings** and select the tabbed form you wish to configure.
Associating an Alias to a Port

To specify an alias parameter to associate a name 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. The system displays the Modify Selected Port form:

   ![Modify Selected Port Form]

   *The General tabbed form varies according to what you have previously selected from the main **Physical Ports** form. The **Alias** field, for example, would not have displayed if you selected the **Modify All Ports** button.*

3. From the **Alias** field, enter the port alias using one or more strings separated by spaces.
4. Click on the **Apply Changes** button to save your configuration.
Ports > Physical Ports > General Port

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.

The system invokes the General tabbed form:

```
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.
Data Size | The number of data bits.
Stop Bits | The number of port stop bits.
Parity | Port parity -- none, even, or odd.
Flow Control | Choices: None, Hardware, or Software.
```

2. Complete the form as follows:

3. Click on the Apply Changes button at the bottom of the ACS configuration window to save your port settings.
Power Management Access

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**.
   The system invokes new fields for selecting the connection type.
3. From the invoked dropdown entry field (**Allow Access by**), select the desired connection type.

The system activates the **Access** and **Other** tabs.

4. If you selected SSH and/or Telnet, select the **Access** tab.
5. From the **Access** tabbed form, configure the authentication method for SSH and/or Telnet, as selected from the previous form.
6. If Biometric authentication is required, select and complete the **Other** tabbed form.
7. Click on **Apply Changes** to save your configuration to Flash.
Ports > Physical Ports > Access

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>
<thead>
<tr>
<th>Authentication Type</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>No authentication.</td>
</tr>
<tr>
<td>Local</td>
<td>Authentication is performed locally (i.e., using the /etc/passwd file).</td>
</tr>
<tr>
<td>Remote</td>
<td>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.</td>
</tr>
<tr>
<td>Radius</td>
<td>Authentication is performed using a Radius authentication server.</td>
</tr>
<tr>
<td>TacacsPlus</td>
<td>Authentication is performed using a TacacsPlus authentication server.</td>
</tr>
<tr>
<td>Ldap</td>
<td>Authentication is performed against an ldap database using an ldap server.</td>
</tr>
<tr>
<td>Kerberos</td>
<td>Authentication is performed using a Kerberos server.</td>
</tr>
<tr>
<td>Local/Radius</td>
<td>Authentication is performed locally first, switching to Radius if unsuccessful.</td>
</tr>
<tr>
<td>Radius/Local</td>
<td>The opposite of the previous option.</td>
</tr>
<tr>
<td>Local/TacacsPlus</td>
<td>Authentication is performed locally first, switching to TacacsPlus if unsuccessful.</td>
</tr>
<tr>
<td>TacacsPlus/Local</td>
<td>The opposite of the previous option.</td>
</tr>
<tr>
<td>RadiusDownLocal</td>
<td>Local authentication is tried only when the Radius server is down.</td>
</tr>
<tr>
<td>TacacsPlusDownLocal</td>
<td>Local authentication is tried only when the TacacsPlus server is down.</td>
</tr>
<tr>
<td>kerberosDownLocal</td>
<td>Local authentication is tried only when the kerberos server is down.</td>
</tr>
<tr>
<td>ldapDownLocal</td>
<td>Local authentication is tried only when the ldap server is down.</td>
</tr>
</tbody>
</table>
To configure user/group authentication, perform the following steps:

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:

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

<table>
<thead>
<tr>
<th>Field Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authorized Users/Groups</td>
</tr>
<tr>
<td>First Authentication Server (Hostname)</td>
</tr>
<tr>
<td>Second Authentication Server (Hostname)</td>
</tr>
<tr>
<td>First Accounting Server (Hostname)</td>
</tr>
<tr>
<td>Second Accounting Server (Hostname)</td>
</tr>
<tr>
<td>Secret</td>
</tr>
<tr>
<td>Timeout</td>
</tr>
<tr>
<td>Retries</td>
</tr>
</tbody>
</table>

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 only when the LDAP server is down.

<table>
<thead>
<tr>
<th>Field Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAP Server</td>
</tr>
<tr>
<td>LDAP Base Domain Name</td>
</tr>
<tr>
<td>Secure LDAP</td>
</tr>
</tbody>
</table>
4: Configuring the Web Interface

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

<table>
<thead>
<tr>
<th>Field Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authorized Users/Groups</td>
</tr>
<tr>
<td>NIS Domain Name</td>
</tr>
<tr>
<td>NIS Server IP</td>
</tr>
</tbody>
</table>

**Authentication Type: Kerberos, KerberosDownLocal**

- **Kerberos**
  - The server performing the authentication.
- **KerberosDownLocal**
  - Local authentication is tried only when the kerberos server is down.

<table>
<thead>
<tr>
<th>Field Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authorized Users/Groups</td>
</tr>
<tr>
<td>Kerberos Server (Realm)</td>
</tr>
<tr>
<td>Kerberos Realm</td>
</tr>
<tr>
<td>Domain Name</td>
</tr>
</tbody>
</table>
4: Configuring the Web Interface

**Ports > Physical Ports > 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:

![Data Buffering Form](image)

2. Complete the necessary fields as follows:

<table>
<thead>
<tr>
<th><strong>Field Name</strong></th>
<th><strong>Definition</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Destination</strong></td>
<td>Select whether the destination of the data buffer is Local or Remote.</td>
</tr>
<tr>
<td><strong>Mode</strong></td>
<td>Select whether the Buffering Mode is Linear (sequential) or Circular (non-sequential).</td>
</tr>
<tr>
<td><strong>Full Size (Bytes)</strong></td>
<td>The maximum limit of the data buffer.</td>
</tr>
<tr>
<td><strong>Record the timestamp...</strong></td>
<td>Commands the system to include a timestamp in the data buffering file.</td>
</tr>
<tr>
<td><strong>Show Menu</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Syslog Fields</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Syslog Server</strong></td>
<td>The IP address of the Syslog Server.</td>
</tr>
<tr>
<td><strong>Facility Number</strong></td>
<td>Facility or location ID of the Syslog Server.</td>
</tr>
</tbody>
</table>
4: Configuring the Web Interface

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.**

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.

**Ports > Physical Ports > 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.

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.
   The system invokes the Multi-User form:

4. Complete the form as follows:

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

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).
Ports > Physical Ports > 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.

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:

   ![Power Management Form](image)

2. Complete the form as follows:

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Power Management on this Port</td>
<td>Check mark to enable Power Management on the selected port(s).</td>
</tr>
<tr>
<td>Power Management Port</td>
<td>View listbox for the PM ports and the assigned outlet numbers.</td>
</tr>
<tr>
<td>Power Management Key</td>
<td>The key sequence which the allowed user(s) can use to perform power management.</td>
</tr>
<tr>
<td>Allow All Users</td>
<td>Radio button to allow all users to perform power management on this port.</td>
</tr>
<tr>
<td>Allow Users/Groups</td>
<td>Radio button to allow only selected users or groups to perform power management on this port.</td>
</tr>
</tbody>
</table>

   ![Field Name and Definition Table](image)
3. Select the **Apply Changes** button at the bottom of the ACS configuration window to save your configuration.

### Ports > Physical Ports > Other

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.

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**:

![](image)

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

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port IP Alias</td>
<td>The IP alias of the selected port.</td>
</tr>
<tr>
<td>TCP Port</td>
<td>The TCP Port number.</td>
</tr>
<tr>
<td>Port Name</td>
<td>As indicated.</td>
</tr>
<tr>
<td>Windows EMS</td>
<td>Checkbox to enable Windows EMS (Expanded Memory).</td>
</tr>
</tbody>
</table>
### 4: Configuring the Web Interface

**Ports > Virtual Ports**

You can use one AlterPath console server as a Master to control other AlterPath console servers (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 **Physical Ports**.

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

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP Keep-alive Interval</td>
<td>Specifies the time interval between the periodic polling by the system to check client processes and connectivity.</td>
</tr>
<tr>
<td>Idle Timeout</td>
<td>The maximum time (in seconds) that a session can be idle before the user is logged off.</td>
</tr>
<tr>
<td>STTY Options</td>
<td>Set terminal options.</td>
</tr>
<tr>
<td>Break Interval</td>
<td>Break interval in milliseconds.</td>
</tr>
<tr>
<td>Login Banner</td>
<td>Text entry field box. Enter the text you wish to appear as a login banner upon logging onto the terminal.</td>
</tr>
<tr>
<td>Host to Connect</td>
<td>Address of the host connected to the port.</td>
</tr>
<tr>
<td>Terminal Type</td>
<td>As indicated.</td>
</tr>
<tr>
<td>Modem Initialization</td>
<td>Text entry field box.</td>
</tr>
<tr>
<td>PPP Options</td>
<td>Options when using this protocol.</td>
</tr>
</tbody>
</table>
2. To add a new slave, select the **Add** button
   - OR -
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:

3. Complete the dialog box as follows:

<table>
<thead>
<tr>
<th><strong>Field Name</strong></th>
<th><strong>Definition</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Number of Ports</strong></td>
<td>Choices are 1, 4, 8, 16, 32 and 48.</td>
</tr>
<tr>
<td><strong>First Local Port No.</strong></td>
<td>As indicated.</td>
</tr>
<tr>
<td><strong>Local IP</strong></td>
<td>Local IP address.</td>
</tr>
<tr>
<td><strong>First Local TCP Port No.</strong></td>
<td>As indicated.</td>
</tr>
<tr>
<td><strong>Remote IP</strong></td>
<td>Remote IP address.</td>
</tr>
<tr>
<td><strong>First Remote TCP Port No.</strong></td>
<td>As indicated.</td>
</tr>
<tr>
<td><strong>Protocol</strong></td>
<td>Communication method between master and slave (Telnet or SSH).</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Port #</th>
<th>Port Name</th>
<th>Local IP</th>
<th>Local TCP Port</th>
<th>Remote IP</th>
<th>Remote TCP Port</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>12</td>
<td></td>
<td>10.10.10.10</td>
<td>0</td>
<td>30.30.30.30</td>
<td>0</td>
<td>telnet</td>
</tr>
<tr>
<td>13</td>
<td></td>
<td>10.10.10.10</td>
<td>1</td>
<td>30.30.30.30</td>
<td>1</td>
<td>telnet</td>
</tr>
<tr>
<td>14</td>
<td></td>
<td>10.10.10.10</td>
<td>2</td>
<td>30.30.30.30</td>
<td>2</td>
<td>telnet</td>
</tr>
<tr>
<td>15</td>
<td></td>
<td>10.10.10.10</td>
<td>3</td>
<td>30.30.30.30</td>
<td>3</td>
<td>telnet</td>
</tr>
<tr>
<td>16</td>
<td></td>
<td>10.10.10.10</td>
<td>4</td>
<td>30.30.30.30</td>
<td>4</td>
<td>telnet</td>
</tr>
<tr>
<td>17</td>
<td></td>
<td>10.10.10.10</td>
<td>5</td>
<td>30.30.30.30</td>
<td>5</td>
<td>telnet</td>
</tr>
<tr>
<td>18</td>
<td></td>
<td>10.10.10.10</td>
<td>6</td>
<td>30.30.30.30</td>
<td>6</td>
<td>telnet</td>
</tr>
<tr>
<td>19</td>
<td></td>
<td>10.10.10.10</td>
<td>7</td>
<td>30.30.30.30</td>
<td>7</td>
<td>telnet</td>
</tr>
<tr>
<td>20</td>
<td></td>
<td>10.10.10.10</td>
<td>8</td>
<td>30.30.30.30</td>
<td>8</td>
<td>telnet</td>
</tr>
<tr>
<td>21</td>
<td></td>
<td>10.10.10.10</td>
<td>9</td>
<td>30.30.30.30</td>
<td>9</td>
<td>telnet</td>
</tr>
<tr>
<td>22</td>
<td></td>
<td>10.10.10.10</td>
<td>10</td>
<td>30.30.30.30</td>
<td>10</td>
<td>telnet</td>
</tr>
<tr>
<td>23</td>
<td></td>
<td>10.10.10.10</td>
<td>11</td>
<td>30.30.30.30</td>
<td>11</td>
<td>telnet</td>
</tr>
<tr>
<td>24</td>
<td></td>
<td>10.10.10.10</td>
<td>12</td>
<td>30.30.30.30</td>
<td>12</td>
<td>telnet</td>
</tr>
<tr>
<td>25</td>
<td></td>
<td>10.10.10.10</td>
<td>13</td>
<td>30.30.30.30</td>
<td>13</td>
<td>telnet</td>
</tr>
<tr>
<td>26</td>
<td></td>
<td>10.10.10.10</td>
<td>14</td>
<td>30.30.30.30</td>
<td>14</td>
<td>telnet</td>
</tr>
<tr>
<td>27</td>
<td></td>
<td>10.10.10.10</td>
<td>15</td>
<td>30.30.30.30</td>
<td>15</td>
<td>telnet</td>
</tr>
</tbody>
</table>

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

**Deleting 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 > Ports Status**

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

<table>
<thead>
<tr>
<th>#</th>
<th>Disable</th>
<th>Alias</th>
<th>Connection Protocol</th>
<th>Serial Config</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td>Console (SSH)</td>
<td>9600 B11</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td>Console (SSH)</td>
<td>9600 B11</td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td>Console (SSH)</td>
<td>9600 B11</td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td>Console (SSH)</td>
<td>9600 B11</td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
<td>Console (SSH)</td>
<td>9600 B11</td>
</tr>
<tr>
<td>6</td>
<td></td>
<td></td>
<td>Console (SSH)</td>
<td>9600 B11</td>
</tr>
<tr>
<td>7</td>
<td></td>
<td></td>
<td>Console (SSH)</td>
<td>9600 B11</td>
</tr>
<tr>
<td>8</td>
<td></td>
<td></td>
<td>Console (SSH)</td>
<td>9600 B11</td>
</tr>
<tr>
<td>9</td>
<td></td>
<td></td>
<td>Console (SSH)</td>
<td>9600 B11</td>
</tr>
<tr>
<td>10</td>
<td></td>
<td></td>
<td>Console (SSH)</td>
<td>9600 B11</td>
</tr>
<tr>
<td>11</td>
<td></td>
<td></td>
<td>Console (SSH)</td>
<td>9600 B11</td>
</tr>
<tr>
<td>12</td>
<td></td>
<td></td>
<td>Console (SSH)</td>
<td>9600 B11</td>
</tr>
<tr>
<td>13</td>
<td></td>
<td></td>
<td>Console (SSH)</td>
<td>9600 B11</td>
</tr>
<tr>
<td>14</td>
<td></td>
<td></td>
<td>Console (SSH)</td>
<td>9600 B11</td>
</tr>
<tr>
<td>15</td>
<td></td>
<td></td>
<td>Console (SSH)</td>
<td>9600 B11</td>
</tr>
<tr>
<td>16</td>
<td></td>
<td></td>
<td>Console (SSH)</td>
<td>9600 B11</td>
</tr>
</tbody>
</table>
Administration

Administration > System Information

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

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

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:

2. Complete the main form as follows:

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Notification Alarm for Data Buffering</strong></td>
<td>Checkmark to enable notification alarms for data buffering.</td>
</tr>
<tr>
<td>[unlabeled view table]</td>
<td>List of alarm types and triggers.</td>
</tr>
<tr>
<td>[unlabeled dropdown list]</td>
<td>Pull-down menu of notification methods (select: Email, Pager, or SNMP Trap).</td>
</tr>
</tbody>
</table>

3. Select the Add button.

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 Notification

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

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

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

![Notifications Entry](image)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alarm Trigger</td>
<td>The trigger expression used to generate an alarm.</td>
</tr>
<tr>
<td>Pager Number</td>
<td>The pager number of the notification recipient.</td>
</tr>
<tr>
<td>Text</td>
<td>The text message for the pager.</td>
</tr>
<tr>
<td>SMS Server IP</td>
<td>The IP address of the SMS server.</td>
</tr>
<tr>
<td>SMS Port</td>
<td>The port used by the SMS server.</td>
</tr>
</tbody>
</table>
SNMP Trap Notification

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:
4. After selecting and completing the Notification Entry dialog box, select the OK button.

5. Select the Apply Changes button at the bottom of the ACS configuration window to save your configuration.

**Port DCD 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 DCD
4. Configure the parameters of the action
5. Select Apply Changes
Administration > 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:

   ![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.
NTP Setting

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

3. Click on the Apply Changes button.
Administration > 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:

![Boot Configuration Form]

2. Complete the fields as follows:

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address assigned to Ethernet</td>
<td>As indicated.</td>
</tr>
<tr>
<td>Watchdog Timer</td>
<td>Sets the Watchdog Timer to Active or Inactive.</td>
</tr>
</tbody>
</table>
### Field Name | Definition
---|---
Unit boot from | Specify whether to boot unit up from Flash or from the Network.
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.
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.
**Administration > 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 a FTP server**

1. From the top menu, select **Administration**; from the left menu, select **Backup Configuration**.
   
The system brings up the **Backup Configuration** form:

2. Complete the form as follows:

<table>
<thead>
<tr>
<th><strong>Field Name</strong></th>
<th><strong>Definition</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Type</strong></td>
<td>Type of backup: FTP or Storage Device.</td>
</tr>
<tr>
<td><strong>Server IP</strong></td>
<td>IP address of the FTP server.</td>
</tr>
<tr>
<td><strong>Path and Filename</strong></td>
<td>Path and filename of the FTP server.</td>
</tr>
<tr>
<td><strong>Username</strong></td>
<td>Username of the person who is doing the backup.</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>Password associated with the Username.</td>
</tr>
</tbody>
</table>
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 AlterPath ACS to display a “DONE” result even though the FTP did not store a copy.
To Save Configuration to a Storage Device

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 Reference 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:

   ![Backup Configuration Form]

3. Complete the form as follows:

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Configuration</td>
<td>The system uses the configuration in the storage device but does not override the internal flash configuration after reboot.</td>
</tr>
<tr>
<td>Replace Configuration</td>
<td>The system saves the configuration in the storage device with a flag REPLACE that is used by the RESTORECONF utility.</td>
</tr>
</tbody>
</table>

4. Click on Save.

5. Click on Apply Changes.
Administration > 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:

1. Select Administration from the top menu, and then select Upgrade Firmware from the left menu.
   
The system brings up the Upgrade Firmware form:

2. Complete the form as follows:

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

3. Click on Upgrade Now.
**Administration > Reboot**

The Reboot form allows you to reboot the system by clicking the Reboot button.
A: **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 100-240V AC, 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™
## Supported PCMCIA Cards

<table>
<thead>
<tr>
<th>Brand</th>
<th>Model</th>
<th>Firmware</th>
</tr>
</thead>
<tbody>
<tr>
<td>10/100BT Ethernet</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Linksys</td>
<td>EtherFast 10/100 PC Card Model PCM100 v3</td>
<td>2.1.0 or higher</td>
</tr>
<tr>
<td>Linksys</td>
<td>EtherFast 10/100 PC Card ver.3</td>
<td>2.1.5 or higher</td>
</tr>
<tr>
<td>D-Link</td>
<td>EtherFast 10/100 PC Card Model DFE-670TXD</td>
<td>2.1.6 or higher</td>
</tr>
<tr>
<td>Fiber Optic</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Danpex</td>
<td>1300C FX100BT (AFC1300SC/ST models)</td>
<td>2.3.0 or higher</td>
</tr>
<tr>
<td>802.11b Wireless Ethernet</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Linksys</td>
<td>WPC11 v.3</td>
<td>2.1.5 or higher</td>
</tr>
<tr>
<td>V.90 (56k) Modem</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Xircom</td>
<td>XM5600 56K PC Card Modem Adapter</td>
<td>2.1.5 or higher</td>
</tr>
<tr>
<td>Zoom</td>
<td>Modem V.92 PC Card Plus Model 3075</td>
<td>2.1.0 or higher</td>
</tr>
<tr>
<td>ISDN</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AVM Fritz!</td>
<td>Card PCMCIA</td>
<td>2.1.1 or higher</td>
</tr>
<tr>
<td>Sedlbauer</td>
<td>Sedlbauer ISDN card</td>
<td>2.1.5 or higher</td>
</tr>
<tr>
<td>GSM</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Novatel Wireless¹</td>
<td>Merlin G201</td>
<td>2.1.4 or higher</td>
</tr>
<tr>
<td>Sierra Wireless¹</td>
<td>AirCard 750</td>
<td>2.1.4 or higher</td>
</tr>
<tr>
<td>Compact Flash²</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hama</td>
<td>64MB CF Memory</td>
<td>2.1.5 or higher</td>
</tr>
<tr>
<td>Kingston</td>
<td>128MB CF Memory</td>
<td>2.1.5 or higher</td>
</tr>
<tr>
<td>PQI</td>
<td>64MB CF Memory</td>
<td>2.1.5 or higher</td>
</tr>
<tr>
<td>SanDisk</td>
<td>64MB CF Memory</td>
<td>2.1.5 or higher</td>
</tr>
<tr>
<td>Aved</td>
<td>16MB CF Memory</td>
<td>2.1.5 or higher</td>
</tr>
<tr>
<td>Other</td>
<td>Most other adapters and compact flash should</td>
<td>2.1.5 or higher</td>
</tr>
<tr>
<td></td>
<td>also work but have not been verified by Cyclades.</td>
<td></td>
</tr>
</tbody>
</table>

1. WARNING: Consult with your local GSM service provider for coverage areas and support of this card prior to using it with the AlterPath™ ACS or ACS1
2. In order to load a Compact Flash card on the AlterPath™ ACS or ACS1, use a PCMCIA Compact Flash adapter.
| IDE Hard Disk   | Toshiba MK5002MPL 5GB | 2.1.5 or higher |
Appendix A: Hardware Specifications
B: Safety Guidelines

This appendix section lists the safety guidelines for:

- RackMounting the ACS
- Operating the ACS

Safety Guidelines for Rack-Mounting the ACS

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

Temperature
The manufacturer's maximum recommended ambient temperature for the AlterPath 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.
Appendix B: Safety Guidelines

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.

DANGER!
Do not operate your ACS with the cover removed.

DANGER!
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.

DANGER!
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.

Important!
To help protect the ACS from electrical power fluctuations, use a surge suppressor, line conditioner, or uninterruptible power supply.

Important!
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.

Important!
Do not spill food or liquids on the ACS.
DANGER!
Do not push any objects through the openings of the ACS. Doing so can cause fire or electric shock by shorting out interior components.

Important!
Keep your ACS away from heat sources and do not block host’s cooling vents.

Important!
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 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 Console Server off.
2. Ground yourself by touching an unpainted metal surface on the back of the equipment before touching anything inside it.
Appendix B: Safety Guidelines

Replacing the Battery

WARNING:
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.

WARNUNG:

FCC Warning Statement

The AlterPath 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 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 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 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 Console Server.

- **¡Peligro!** No hacer funcionar el AlterPath Console Server con la tapa abierta.

- **¡Peligro!** Para prevenir un corto circuito en el AlterPath 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.

- **¡Peligro!** 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.

- **¡Importante!** Para proteger al AlterPath Console Server de fluctuaciones en corriente eléctrica, utilice una fuente eléctrica de respaldo.

- **¡Importante!** Asegurarse de que nada descanse sobre los cables del AlterPath Console Server, y que los cables no obstruyan el paso.

- **¡Importante!** Asegurarse de no dejar caer alimentos o bebidas en el AlterPath Console Server. Si esto ocurre, avise a Cyclades Corporation.

- **¡Peligro!** No empuje ningún tipo de objeto en los compartimentos del AlterPath Console Server. Hacer esto podría ocasionar un incendio o causar un corto circuito dentro del equipo.
¡Importante! Mantenga el AlterPath Console Server Cyclades-TS fuera del alcance de calentadores, y asegurarse de no tapar la ventilación del equipo.


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 Console Server. El límite mínimo del interruptor deberá ser 2 amperes, con conductor de 0.75 mm (18 AWG).

**Trabajar dentro del AlterPath Console Server**

No intente dar servicio al AlterPath 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 Console Server. Asegurase que este tocando tierra antes de tocar cualquier otra cosa, que puede ser al tocar la parte trasera del equipo.

**Batería**

¡Peligro! Una batería nueva puede explotar, si no esta instalada correctamente. Remplace 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.
C: Supported Browsers and JRE

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 Environment

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

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.

From Windows Internet Explorer

Go to Tools > Internet Options > Advanced. Scroll down and look for a section on Java. There should be a checkbox 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.

**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

<table>
<thead>
<tr>
<th><strong>Authentication</strong></th>
<th>The process by which a user’s identity is checked within the network to ensure that the user has access to the requested resources.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Basic In/Out System (BIOS)</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Baud Rate</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Boot</strong></td>
<td>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).</td>
</tr>
<tr>
<td><strong>Break Signal</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Checksum</strong></td>
<td>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</td>
</tr>
</tbody>
</table>
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.

**Hot-Swap**

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

**ICMP**

*Internet Control Message Protocol* 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 *packets*), 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 *IP Security Protocol*, 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.

**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 keepalive 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.
Glossary

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).