Cyclades-TS Version TS 1.4.0
November 25th, 2004
Copyright © Cyclades Corporation, 2004

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 v1.3.12. All brand and product names mentioned in this publication are trademarks or registered trademarks of their respective holders.

Cyclades, Cyclades-TS3000, Cyclades-TS2000, Cyclades-TS1000, Cyclades-TS800, Cyclades-TS400, Cyclades-TS110, and Cyclades-TS100 are registered trademark of Cyclades Corporation.
Microsoft, Windows 95, 98, XP, ME, NT, and 2K are trademarks of Microsoft Corporation.

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.

Document Number TS 1.4.0 - revision 1
# Table of Contents

## Preface

- Purpose ................................................................. 11
- Audience and User Levels ........................................ 11
  - New Users ......................................................... 11
  - Power Users ..................................................... 11
- How to use this Guide .............................................. 12
- Additional Documentation and Help .............................. 13
- Conventions and Symbols ........................................ 13
  - Fonts ................................................................. 13
  - Hypertext Links .................................................. 14
  - Glossary Entries ................................................ 14
  - Quick Steps ....................................................... 14
  - Parameter Syntax ................................................ 15
  - Note Box Icons ................................................... 17

## Chapter 1 - Introduction and Overview

- Introducing Cyclades ................................................ 19
- The Cyclades-TS ..................................................... 19
- What’s in the box ..................................................... 20
  - Powering the TS110/100 .......................................... 29
  - Power Supply Installation ....................................... 29
- Safety Instructions .................................................. 31
  - Replacing the Battery ............................................ 33
- Federal Communications Commission & Industry Canada Radio Frequency Interference Statements ........................................ 34
- Notice about FCC compliance for the Cyclades-TS1000 and the Cyclades-TS2000 34
- Normas Oficiales Mexicanas (NOM) Electrical Safety Statement .......... 34
- Aviso de Precaución S-Mark Argentina ............................. 36
- Trabajar dentro del Cyclades-TS ................................. 38
- Batería ................................................................. 38

## Chapter 2 - Installation, Configuration, and Usage

- Introduction ............................................................ 39
- System Requirements ................................................ 39
- Default Configuration Parameters ................................ 40
- Pre-Install Checklist .................................................. 41
# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Task List</td>
<td>42</td>
</tr>
<tr>
<td>The Wizard</td>
<td>42</td>
</tr>
<tr>
<td>Quick Start</td>
<td>44</td>
</tr>
<tr>
<td>Configuration using a Console</td>
<td>44</td>
</tr>
<tr>
<td>Configuration using a Web browser</td>
<td>47</td>
</tr>
<tr>
<td>Configuration using Telnet</td>
<td>55</td>
</tr>
<tr>
<td>The Installation and Configuration Process</td>
<td>58</td>
</tr>
<tr>
<td>Task 1: Connect the Cyclades-TS to the Network and other Devices</td>
<td>58</td>
</tr>
<tr>
<td>Task 2: Configure the COM Port Connection and Log In</td>
<td>61</td>
</tr>
<tr>
<td>Task 3: Modify the System Files</td>
<td>63</td>
</tr>
<tr>
<td>Task 4: Edit the pslave.conf file</td>
<td>66</td>
</tr>
<tr>
<td>Task 5: Activate the changes</td>
<td>69</td>
</tr>
<tr>
<td>Task 6: Test the configuration</td>
<td>69</td>
</tr>
<tr>
<td>Task 7: Save the changes</td>
<td>70</td>
</tr>
<tr>
<td>Task 8: Reboot the Cyclades-TS</td>
<td>70</td>
</tr>
<tr>
<td>Special Configuration for the Cyclades-TS110/100</td>
<td>71</td>
</tr>
<tr>
<td>TS110/100-specific background information.</td>
<td>71</td>
</tr>
<tr>
<td>Configuring the Cyclades-TS110/100 for the first time</td>
<td>72</td>
</tr>
<tr>
<td>Accessing the Serial Ports</td>
<td>74</td>
</tr>
<tr>
<td>Opening and closing a telnet session to a serial port</td>
<td>74</td>
</tr>
<tr>
<td>Opening and closing an SSH session to a serial port</td>
<td>74</td>
</tr>
<tr>
<td>Accessing Serial Ports using “ts_menu”</td>
<td>75</td>
</tr>
</tbody>
</table>

## Chapter 3 - Additional Features

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>77</td>
</tr>
<tr>
<td>Configuration Wizard - Basic Wizard</td>
<td>78</td>
</tr>
<tr>
<td>Using the Wizard through your Browser</td>
<td>84</td>
</tr>
<tr>
<td>Access Method</td>
<td>86</td>
</tr>
<tr>
<td>Configuration for CAS</td>
<td>86</td>
</tr>
<tr>
<td>Configuration for TS</td>
<td>101</td>
</tr>
<tr>
<td>Configuration for Dial-in Access</td>
<td>109</td>
</tr>
<tr>
<td>Authentication</td>
<td>114</td>
</tr>
<tr>
<td>Parameters Involved and Passed Values</td>
<td>114</td>
</tr>
<tr>
<td>Configuration for CAS, TS, and Dial-in Access</td>
<td>116</td>
</tr>
<tr>
<td>Access Control via Radius Attribute NAS-Port-id</td>
<td>125</td>
</tr>
<tr>
<td>CAS Port Pool</td>
<td>126</td>
</tr>
<tr>
<td>How to Configure it</td>
<td>127</td>
</tr>
<tr>
<td>Centralized Management</td>
<td>129</td>
</tr>
<tr>
<td>Clustering</td>
<td>133</td>
</tr>
</tbody>
</table>
# Table of Contents

- Parameters Involved and Passed Values .............................................. 134
- CronD ................................................................. 138
  Parameters Involved and Passed Values .............................................. 138
  Configuration for CAS, TS, and Dial-in Access .................................. 139
- Data Buffering ................................................................. 140
  Introduction ............................................................................... 140
  Linear vs. Circular Buffering .......................................................... 141
  Parameters Involved and Passed Values .............................................. 141
  Configuration for CAS ................................................................. 144
- DHCP ................................................................. 155
  Parameter Involved and Passed Values ............................................... 155
  Configuration for CAS, TS, and Dial-in Access .................................. 157
- Filters ................................................................. 159
  Description ............................................................................... 159
  Configuration for CAS, TS, and Dial-in Access .................................. 160
- Generating Alarms ................................................................. 162
  Port Slave Parameters Involved with Generating Alarms ...................... 162
  Configuration for CAS, TS, and Dial-in Access .................................. 162
  Syslog-ng Configuration to use with Alarm Feature ......................... 169
  Alarm, Sendmail, Sendsms and Snmptrap .......................................... 171
- Help ................................................................. 178
  Help Wizard Information .............................................................. 178
  Help Command Line Interface Information ...................................... 179
- Modbus ................................................................. 185
- NTP ................................................................. 187
  Parameters Involved and Passed Values .............................................. 187
  Configuration for CAS, TS, and Dial-in Access .................................. 188
- Ports Configured as Terminal Servers .............................................. 189
  TS Setup Wizard ......................................................................... 189
- Serial Settings ................................................................. 195
  Parameters Involved and Passed Values .............................................. 195
  Configuration for CAS ................................................................. 196
  CLI Method ............................................................................... 204
  Configuration for TS ..................................................................... 205
  Configuration for Dial-in Access ...................................................... 209
- Session Sniffing ........................................................................... 211
  Versions 1.3.2 and earlier ............................................................... 211
  Versions 1.3.3 and later .................................................................... 212
  Parameters Involved and Passed Values .............................................. 215
  Configuration for CAS ................................................................. 216
## Table of Contents

SNMP ................................................................. 226
Syslog .................................................................. 232
  Port Slave Parameters Involved with syslog-ng ............. 233
  Configuration for CAS, TS, and Dial-in Access ................. 233
  The Syslog Functions ........................................... 239
TCP Keepalive ....................................................... 253
  How it works .................................................... 253
  How to Configure it ............................................ 254
Terminal Appearance ............................................... 255
  Parameters Involved and Passed Values ......................... 255
  Configuration for CAS, TS, and Dial-in Access ................. 256
Time Zone .............................................................. 264
  How to set Date and Time ...................................... 265
  Automatically adjust for Daylight Savings Time: ............... 265
TS110-only Analog and Digital Ports ............................. 267
  Digital Ports ...................................................... 267
  Analog Ports ...................................................... 267
  Port Utility (/bin/pu) ........................................... 267
  Analog and Digital ports on the Web ........................... 269
Sending Warning Messages ........................................ 269
Linux-PAM ........................................................... 272
  The Linux-PAM Configuration File ............................ 274
    Configuration File Syntax .................................... 274
    Module Path ...................................................... 276
    Arguments ...................................................... 279
LDAP Authentication ............................................... 281
  LDAP server for Linux .......................................... 281
  Default Policy .................................................. 285
  Reference ......................................................... 292
Power Management ................................................. 293
  Configuration ..................................................... 293
    Port Slave Parameters Involved and Passed Values .......... 294
    Syslog Messages Generated by the IPDU ...................... 295
    How to change the IPDU Password ............................ 296
    vi Method ...................................................... 296
    Browser Method .............................................. 297
    Wizard Method ............................................... 298
  How to Access the AlterPath PM regular menu from the Console Session 301
  Power Management for the Authorized Users (firmware version prior to 1.4.0) 305
Table of Contents

Adding an user of the pmusers group ........................................ 305
Changing the group of an already existing user ...................... 305
pm command ................................................................. 306
pmCommand command ...................................................... 309
AlterPath PM Firmware Upgrade ........................................ 311
Upgrade Process ............................................................. 311
Power Management from a Browser ..................................... 313
Menu Shell ................................................................. 316
  How to use .............................................................. 316
  How to configure ...................................................... 316
SNMP Proxy .............................................................. 317
  How to Configure ..................................................... 318
Start and Stop Daemons .................................................. 320
  How to Configure Them .............................................. 322

Appendix A - New User Background Information

Users and Passwords ..................................................... 325
How to show who is logged in and what they are doing .......... 326
Linux File Structure .................................................... 326
Basic File Manipulation Commands .................................. 327
The vi Editor .............................................................. 328
The Routing Table ....................................................... 331
Secure Shell Session .................................................... 332
  The Session Channel Break Extension ............................ 334
The Process Table ........................................................ 337
TS Menu Script .......................................................... 338

Appendix B - Cabling, Hardware, and Electrical Specifications

General Hardware Specifications ....................................... 343
The RS-232 Standard ....................................................... 345
Cable Length .............................................................. 346
Connectors ................................................................. 347
Straight-Through vs. Crossover Cables ............................... 348
Which cable should be used? .......................................... 348
Cable Diagrams ........................................................... 349
TS110/100-only Cabling Information ................................ 355
  The RS-485 Standard .................................................. 355
  TS110/100 Connectors ................................................ 355
# Table of Contents

TS110 Current Specifications .............................................. 356  
Cable Diagrams ............................................................. 357  

## Appendix C - The pslave Configuration File

Introduction ................................................................. 361  
Configuration Parameters ................................................ 361  
CAS, TS, and Dial-in Common Parameters .............................. 361  
CAS Parameters ............................................................ 372  
TS Parameters ............................................................. 383  
Dial-in Access Parameters ............................................... 384  

## Appendix D - Software Upgrades and Troubleshooting

Upgrades ........................................................................... 387  
The Upgrade Process ......................................................... 387  
Troubleshooting ................................................................ 389  
Flash Memory Loss .......................................................... 389  
Hardware Test ..................................................................... 392  
Port Test .......................................................................... 392  
Port Conversation .............................................................. 393  
Test Signals Manually ......................................................... 393  
Test Analog Ports (for the TS110 only) ............................... 394  
Test Digital Ports (for the TS110 only) ............................... 395  
Single User Mode ............................................................. 395  
Troubleshooting the Web Configuration Manager ............... 397  
What to do when the initial Web page does not appear .......... 397  
How to restore the Default Configuration of the Web Configuration Manager 397  
Using a different speed for the Serial Console .................... 398  
CPU LED ........................................................................ 400  

## Appendix E - Certificate for HTTP Security

Introduction ................................................................. 401  
Procedure ................................................................. 401  

## Appendix F - Web User Management

Introduction ................................................................. 405
# Table of Contents

Default Configuration for Web User Management .................................................. 405
How Web User Management works ................................................................. 407
  Task 1: Check the URL in the Access Limit List ............................................ 407
  Task 2: Read the Username and the Password .............................................. 408
  Task 3: Look for the group retrieved in the user groups list ......................... 408
Web User Management Configuration - Getting Started ............................... 408
  Changing the Root Password ................................................................. 409
Adding and Deleting Users ............................................................................. 409
  Adding a User ......................................................................................... 409
  Deleting a User ...................................................................................... 410
Adding and Deleting User Groups ................................................................. 411
  Adding a group ..................................................................................... 411
  Deleting a group .................................................................................... 411
Adding and Deleting Access Limits ............................................................... 412
  Adding an Access Limit ....................................................................... 412
  Deleting an access limit ..................................................................... 413

Appendix G - Connect to Serial Ports from Web

  Introduction ......................................................................................... 415
  Tested Environment .............................................................................. 415
  On Windows ......................................................................................... 416
  From Internet Explorer ......................................................................... 416
  From Netscape or Mozilla ..................................................................... 416
  Step-by-Step Process .......................................................................... 417

Appendix H - Examples for Configuration Testing

  Introduction ......................................................................................... 421
  Console Access Server ......................................................................... 421
  Terminal Server .................................................................................. 425
  Dial-in Access .................................................................................... 427

Appendix I - Billing Feature

  Introduction ......................................................................................... 429
  General Feature Description .................................................................. 429
  Configuration ....................................................................................... 429
  How it works ....................................................................................... 430
  Billing Configuration Script .................................................................. 431
Table of Contents

Disk Space Issue ................................................................. 432

Appendix J - Wiz Application Parameters

  Basic Parameters (wiz) ...................................................... 433
  Access Method Parameters (wiz -ac <type>) ................................ 433
  Alarm Parameter (wiz -al) ............................................... 434
  Authentication Parameters (wiz -auth) .................................. 434
  Data Buffering Parameters (wiz -db) .................................. 435
  Power Management Parameters (wiz -pm) ............................... 435
  Serial Settings Parameters (wiz -sset <type>) ......................... 436
  Sniffing Parameters (wiz -snf) ........................................ 437
  Syslog Parameters (wiz -sl) ............................................ 437
  Terminal Appearance Parameters (wiz -tl) ............................. 437
  Terminal Server Profile Other Parameters (wiz -tso) .................. 438

Appendix K - Copyrights

  References ................................................................. 439

List of Figures ................................................................. 443

List of Tables ................................................................. 447

Glossary ................................................................. 449

Index ................................................................. 453
Preface

Purpose

The purpose of this guide is to provide instruction for users to independently install, configure, and maintain the Cyclades-TS. This manual should be read in the order written, with exceptions given in the text. *Whether or not you are a UNIX user, we strongly recommend that you follow the steps given in this manual.*

Audience and User Levels

This guide is intended for the user who is responsible for the deployment and day-to-day operation and maintenance of the Cyclades-TS. It assumes that the reader understands networking basics and is familiar with the terms and concepts used in Local and Wide Area Networking. UNIX and Linux users will find the configuration process very familiar. It is not necessary to be a UNIX expert, however, to get the Cyclades-TS up and running. There are two audiences or user levels for this manual:

**New Users**

These are users new to Linux and/or UNIX with a primarily PC/Microsoft background. You might want to brush up on such things as common Linux/UNIX commands and how to use the vi editor prior to attempting installation and configuration. This essential background information appears in Appendix A - New User Background Information. It is recommended that New Users configure the Cyclades-TS using a Web browser, however, New Users can also configure the Cyclades-TS with vi, the Wizard or the Command Line Interface (CLI).

**Power Users**

These are UNIX/Linux experts who will use this manual mostly for reference. Power Users can choose between configuring the Cyclades-TS via Web browser, vi, Wizard, or CLI.

Each configuration task will be separated into a section (a clickable link on the PDF file) for each user type. Users then can skip to the appropriate level that matches their expertise and comfort level.
Preface

How to use this Guide

This guide is organized into the following sections:

- **Chapter 1 - Introduction and Overview** contains an explanation of the product and its default CAS setup. It also includes safety guidelines to be followed.

- **Chapter 2 - Installation, Configuration, and Usage** explains how the Cyclades-TS should be connected and what each cable is used for. It describes the basic configuration process to get the Cyclades-TS up and running for its most common uses.

- **Appendix A - New User Background Information** contains information for those who are new to Linux/UNIX.

- **Appendix B - Cabling, Hardware, and Electrical Specifications** has detailed information and pinout diagrams for cables used with the Cyclades-TS.

- **Appendix C - The pslave Configuration File** contains example files for the various configurations as well as the master file.

- **Appendix D - Software Upgrades and Troubleshooting** includes solutions and test procedures for typical problems.

- **Appendix E - Certificate for HTTP Security** provides configuration information that will enable you to obtain a Signed Digital Certificate.

- **Appendix F - Web User Management** covers default and optional configuration, and the addition/deletion of users, groups, and access limits.

- **Appendix G - Connect to Serial Ports from Web** enables this process, based on how the serial port is configured.

- **Appendix H - Examples for Configuration Testing** provides examples for testing the Cyclades-TS after configuration.

- **Appendix I - Billing Feature** explains how the Cyclades TS family can also be simply used as an intermediate buffer to collect serial data (like billing tickets from a PABX), making them available for a posterior file transfer.

- **Appendix J - Wiz Application Parameters** contains all basic and custom wizard parameters.
Preface

- Appendix K - Copyrights lists details about applications that were incorporated into the product.
- The Glossary provides definitions for commonly-used terms in this manual.

Additional Documentation and Help

There are other Cyclades documents that contain background information about Console Port Management and the Cyclades product line. These are:

- Cyclades’ Console Management in the Data Center
- Cyclades' Product Catalog

For the most updated version of Cyclades' documentation, use the following Web address:

http://www.cyclades.com/support/downloads.php

Technical Support Centers

To reach Cyclades’ Technical Support Centers, go to the following:

http://www.cyclades.com/support/technical_support.php

Conventions and Symbols

This section explains the significance of each of the various fonts, formatting, and icons that appear throughout this guide.

Fonts

This guide uses a regular text font for most of the body text and Courier for data that you would input, such as a command line instruction, or data that you would receive back, such as an error message. An example of this would be:

telnet 200.200.200.1 7001
Hypertext Links

References to another section of this manual are hypertext links that are underlined (and are also blue in the PDF version of the manual). When you click on them in the PDF version of the manual, you will be taken to that section.

Glossary Entries

Terms that can be found in the glossary are underlined and slightly larger than the rest of the text. These terms have a hypertext link to the glossary.

Quick Steps

Step-by-step instructions for installing and configuring the Cyclades-TS are numbered with a summarized description of the step for quick reference. Underneath the quick step is a more detailed description. Steps are numbered 1, 2, 3, etc. Additionally, if there are sub-steps to a step, they are indicated as Step A, B, C, and are nested within the Step 1, 2, 3, etc. For example:
Step 1: Modify files.
You will modify four Linux files to let the Cyclades-TS know about its local environment.

Step A: Modify pslave.conf.
Open the file pslave.conf and add the following lines . . .

Parameter Syntax
This manual uses standard Linux command syntaxes and conventions for the parameters described within it.

Brackets and Hyphens (dashes)
The brackets ([[]]) indicate that the parameter inside them is optional, meaning that the command will be accepted if the parameter is not defined. When the text inside the brackets starts with a dash (-) and/or indicates a list of characters, the parameter can be one of the letters listed within the brackets.

Example:
iptables [-ADC] chain rule-specification [options]

Ellipses
Ellipses (...) indicate that the latest parameter can be repeated as many times as needed. Usually this is used to describe a list of subjects.
Example:

```
ls [OPTION]... [FILE]...
```

**Pipes**

The pipe (|) indicates that one of the words separated by this character should be used in the command.

Example:

```
netstat {--statistics|-s} [--tcp|-t] [--udp|-u] [--raw|-w]
```

When a configuration parameter is defined, the Linux command syntax conventions will be also used, with a difference.

**Greater-than and Less-than signs**

When the text is encapsulated with the “<>” characters, the meaning of the text will be considered, not the literal text. When the text is not encapsulated, the literal text will be considered.

**Spacing and Separators**

The list of users in the following example must be separated by semicolons (;); the outlets should be separated by commas (,) to indicate a list or with dashes (-) to indicate range; there should not be any spaces between the values.

```
sXX.pmusers: The user access list. For example: jane:1,2;john:3,4. The format of this field is:
[<username>:<outlet list>];[<username>:<outlet list>...]
```

where `<outlet list>`’s format is:

```
[<outlet number>|<outlet start>-<outlet end>],<outlet number>|<outlet start>-<outlet end>]
```
Preface

Note Box Icons

Note boxes contain instructional or cautionary information that the reader especially needs to bear in mind. There are five levels of note box icons:

- **Tip.** An informational tip or tool that explains and/or expedites the use of the Cyclades-TS.

- **Important!** An important tip that should be read. Review all of these notes for critical information.

- **Warning!** A very important type of tip or warning. Do not ignore this information.

- **DANGER!** Indicates a direct danger which, if not avoided, may result in personal injury or damage to the system.

- **Security Issue.** Indicates security-related information where it is relevant.
This page has been left intentionally blank.
Chapter 1 - Introduction and Overview

Introducing Cyclades

Cyclades is a data center fault management company that enables remote management of servers, network equipment and automation devices. Its products help data center managers at enterprise, telecommunication and Internet companies to maximize network and server availability. This results in decreased maintenance costs, increased efficiency and productivity, along with greater control, freedom and peace of mind. Cyclades’ advantage is providing scalable products leveraging Linux technology for flexibility and ease of customization.

The Cyclades-TS

The Cyclades-TS is line of Console Access and Terminal Servers that allow both local and dial-in access for in-band and out-of-band network management. They run an embedded version of the Linux operating system. Configuration of the equipment is done by editing a few plaintext files, and then updating the versions of the files on the Cyclades-TS. The files can be edited using the vi editor provided or on another computer with the environment and text editor of your choice. The default “box profile” of the Cyclades-TS is that of a Console Access Server.

You can access the Cyclades-TS via three methods:

- A console directly connected to the Cyclades-TS
- Telnet/ssh over a network
- A browser

And configure it with any of the following four options:

- vi
- Wizard
- Browser
- Command Line Interface (CLI) - only for certain configuration parameters
Chapter 1 - Introduction and Overview

With the Cyclades-TS set up as a Console Access Server, you can access a server connected to the Cyclades-TS through the server's serial console port from a workstation on the LAN or WAN. There is no authentication by default, but the system can be configured for authentication to be performed by a Radius server, a TacacsPlus server, or even by a local database. Either telnet or ssh (a secure shell session) can be used. See Appendix A - New User Background Information for more information about ssh. The instructions in Chapter 2 - Installation, Configuration, and Usage will set up a fully-functional, default CAS environment. More options can be added after the initial setup, as illustrated in Chapter 3 - Additional Features.

What’s in the box

There are several models of the Cyclades-TS with differing numbers of serial ports. Cyclades will ship either Cable Package #1 or #2 with the product according to current availability.

![Figure 1: Cable Package #1](image)

- RJ-45 straight-through cable
- RJ-45 to DB-9 F adapter
- Cyclades/Sun Netra adapter
- RJ-45 to DB-25 Male adapter
- RJ-45 to DB-25 Female adapter
Chapter 1 - Introduction and Overview

The following figures show the main units and accessories included in each package.

Figure 2: Cable Package #2
Chapter 1 - Introduction and Overview

Figure 3: The Cyclades-TS3000 and cables
Chapter 1 - Introduction and Overview

Figure 4: The Cyclades-TS2000 and cables
Chapter 1 - Introduction and Overview

Figure 5: The Cyclades-TS1000 and cables
Chapter 1 - Introduction and Overview

Figure 6: The Cyclades-TS800 and cables
Figure 7: The Cyclades-TS400 and cables
Figure 8: The Cyclades-TS110 and cables
Chapter 1 - Introduction and Overview

Figure 9: The Cyclades-TS100 and cables
Chapter 1 - Introduction and Overview

Powering the TS110/100

There are three ways to supply power to the TS110/100:

1. External AC Desktop Power Supply: Universal AC Input (100-240VAC) / 5VDC Output. This power supply is shipped with the standard TS110/100 unit (AC input)

2. External DC Supply. Three DC input options are available:
   - 12VDC nominal input (9-18 VDC)
   - 24VDC nominal input (18-36 VDC)
   - 48VDC nominal input (36-72 VDC)

3. P.O.E. (Power Over Ethernet)
   The power is supplied through the Ethernet cable. When this option is selected, the TS110/100 unit has to be connected to the LAN through a special hub or switch that provides DC voltage over the LAN cable. Besides these special hubs and switches, there are power injector devices available in the market which allow the users to keep using the regular hubs and switches. There are two P.O.E. standards in terms of P.O.E. feature detection circuitry. The P.O.E. supplier unit (hub, switch or power injector) can detect if the attached device supports P.O.E. One standard (old) uses capacitive load process and the second standard (new) uses resistive load process. TS110/100 supports both standards.

Power Supply Installation

External Desktop AC Power Supply

Step 1: Connect one end of the power cable to the TS110/100 power jack (5VDC in).

Step 2: Connect the power supply end of the power cable to a standard wall outlet.

External DC Supply

Connect the two DC supply wires to the terminal block, marked as PW- and PW+. The positive voltage should be connected to PW+ and the return to PW-. If it is a -48VDC supply, the -48V signal should be connected to PW- and the return signal to PW+.
Chapter 1 - Introduction and Overview

Notes:
- There is a label on the TS110/100 unit showing the nominal DC input voltage.
- The external desktop AC Power Supply (Universal AC input / 5VDC output) is shipped with the TS110/100 as a standard accessory.
- If the 5VDC input power jack is used, it will bypass the DC input from the terminal block.
- There is a protection on the terminal block’s DC input. If the (PW+) and (PW-) signals are inverted, the TS110/100 just won’t work. It does not cause any damage to the unit.

P.O.E. (Power Over Ethernet)
No special setup is required. Just connect the Ethernet cable coming from the hub or switch that has support for P.O.E. or to the power injector device.

Notes: If the 5VDC input power jack is used, it will bypass the P.O.E. feature.
- The external desktop AC Power Supply (Universal AC input / 5VDC output) is not shipped with the TS110/100 as standard accessory.
Chapter 1 - Introduction and Overview

Safety Instructions

Read all the following safety guidelines to protect yourself and your Cyclades-TS.

**DANGER!** Do not operate your Cyclades-TS with the cover removed.

**DANGER!** In order to avoid shorting out your Cyclades-TS when disconnecting the network cable, first unplug the cable from the equipment and then from the network jack. When reconnecting a network cable to the equipment, first plug the cable into the network jack, and then into the equipment.

**DANGER!** To help prevent electric shock, plug the Cyclades-TS 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. For the TS110/100, TS400, and 800, the grounded power cable constraint does not apply, as these products have an external power supply, and one power cable instead of two.

**Important!** To help protect the Cyclades-TS 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 Cyclades-TS and that they are not located where they can be stepped on or tripped over.
Chapter 1 - Introduction and Overview

**Important!** Do not spill food or liquids on the Cyclades-TS. If it gets wet, contact Cyclades.

**DANGER!** Do not push any objects through the openings of the Cyclades-TS. Doing so can cause fire or electric shock by shorting out interior components.

**Important!** Keep your Cyclades-TS away from heat sources and do not block cooling vents.

**Important!** The Cyclades-TS 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 Cyclades-TS DC version. Minimum Breaker Rating: 2A. Required conductor size: 18 AWG.

**Working inside the Cyclades-TS**

Do not attempt to service the Cyclades-TS yourself, except when following instructions from Cyclades Technical Support personnel. In the latter case, first take the following precautions:
Chapter 1 - Introduction and Overview

- Turn the Cyclades-TS off.
- Ground yourself by touching an unpainted metal surface on the back of the equipment before touching anything inside it.

Replacing the Battery

A coin-cell battery maintains date and time information. The TS110/100 does not have the battery, so the date and time must be kept up-to-date by ntpclient.

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

**Предупреждение.** Есть опасность взрыва, если батарея заменена неправильно. Замените батарею только тем же самым или эквивалентным типом, рекомендованным изготовителем. Извиняться от используемых батарей согласно инструкциям изготовителя.
Chapter 1 - Introduction and Overview

Federal Communications Commission & Industry Canada Radio Frequency Interference Statements

This equipment generates, uses, and can radiate radio-frequency energy, and if not installed and used properly, that is, in strict accordance with the manufacturer's instructions, may cause interference to radio communication.

It has been tested and found to comply with the limits for a Class A computing device in accordance with the specifications in Subpart B of Part 15 of FCC rules, which are designed to provide reasonable protection against such interference when the equipment is operated in a commercial environment. Operation of this equipment in a residential area is likely to cause interference, in which case the user at his own expense will be required to take whatever measures may be necessary to correct the interference.

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This digital apparatus does not exceed the Class A limits for radio noise emission from digital apparatus set out in the Radio Interference Regulation of Industry Canada.

Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de classe A prescrites dans le Règlement sur le brouillage radioélectrique publié par Industrie Canada.

Notice about FCC compliance for the Cyclades-TS1000 and the Cyclades-TS2000

In order to comply with FCC standards the Cyclades-TS 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.

Normas Oficiales Mexicanas (NOM) Electrical Safety Statement

Instrucciones de Seguridad

1. Todas las instrucciones de seguridad y operación deberán ser leídas antes de que el aparato eléctrico sea operado.

2. Las instrucciones de seguridad y operación deberán ser guardadas para referencia futura.
3. Todas las advertencias en el aparato eléctrico y en sus instrucciones de operación deben ser respetadas.

4. Todas las instrucciones de operación y uso deben ser seguidas.

5. El aparato eléctrico no deberá ser usado cerca del agua—por ejemplo, cerca de la tina de baño, lavabo, sótano mojado o cerca de una alberca, etc..

6. El aparato eléctrico debe ser usado únicamente con carritos o pedestales que sean recomendados por el fabricante.

7. El aparato eléctrico debe ser montado a la pared o al techo sólo como sea recomendado por el fabricante.

8. Servicio—El usuario no debe intentar dar servicio al equipo eléctrico más allá a lo descrito en las instrucciones de operación. Todo otro servicio deberá ser referido a personal de servicio calificado.

9. El aparato eléctrico debe ser situado de tal manera que su posición no interfiera su uso. La colocación del aparato eléctrico sobre una cama, sofá, alfombra o superficie similar puede bloquear la ventilación, no se debe colocar en libreros o gabinetes que impidan el flujo de aire por los orificios de ventilación.

10. El equipo eléctrico debe ser situado fuera del alcance de fuentes de calor como radiadores, registros de calor, estufas u otros aparatos (incluyendo amplificadores) que producen calor.

11. El aparato eléctrico deberá ser conectado a una fuente de poder sólo del tipo descrito en el instructivo de operación, o como se indique en el aparato.

12. Precaución debe ser tomada de tal manera que la tierra física y la polarización del equipo no sea eliminada.

13. Los cables de la fuente de poder deben ser guiados de tal manera que no sean pisados ni pellizcados por objetos colocados sobre o contra ellos, poniendo particular atención a los contactos y receptáculos donde salen del aparato.

14. El equipo eléctrico debe ser limpiado únicamente de acuerdo a las recomendaciones del fabricante.

15. En caso de existir, una antena externa deberá ser localizada lejos de las líneas de energía.

16. El cable de corriente deberá ser desconectado del cuando el equipo no sea usado por un largo periodo de tiempo.
17. Cuidado debe ser tomado de tal manera que objetos líquidos no sean derramados sobre la cubierta u orificios de ventilación.

18. Servicio por personal calificado deberá ser provisto cuando:
   - El cable de poder o el contacto ha sido dañado; u
   - Objectos han caído o líquido ha sido derramado dentro del aparato; o
   - El aparato ha sido expuesto a la lluvia; o
   - El aparato parece no operar normalmente o muestra un cambio en su desempeño; o
   - El aparato ha sido tirado o su cubierta ha sido dañada.

**Aviso de Precaución S-Mark Argentina**

Por favor de leer todos los avisos de precaución como medida preventiva para el operador y el Cyclades-TS.

**¡Peligro!** No hacer funcionar el Cyclades-TS con la tapa abierta.

**¡Peligro!** Para prevenir un corto circuito en el Cyclades-TS 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 Cyclades-TS de fluctuaciones en corriente eléctrica, utilice una fuente eléctrica de respaldo.

¡Importante! Asegurarse de que nada descanse sobre los cables del Cyclades-TS, y que los cables no obstruyan el paso.

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

¡Peligro! No empuje ningún tipo de objeto en los compartimientos del Cyclades-TS. Hacer esto podría ocasionar un incendio o causar un corto circuito dentro del equipo.

¡Importante! Mantenga el 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 Cyclades-TS. El límite mínimo del interruptor deberá ser 2 amperes, con conductor de 0.75 mm (18 AWG).

Trabajar dentro del Cyclades-TS

No intente dar servicio al Cyclades-TS, solo que este bajo la dirección de Soporte Técnico de Cyclades Corporation. Si este es el caso, tome las siguientes precauciones:

Apague el Cyclades-TS. Asegúrese que esté 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 está 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.
Chapter 2 - Installation, Configuration, Usage

**Introduction**

This chapter will allow you to install and configure the Cyclades-TS as the default CAS configuration. *Please read the entire chapter before beginning*. A basic installation and configuration should take a half hour at the most, either done manually or with the Wizard.

The Cyclades-TS operating system is embedded Linux. If you are fairly new to Linux, you will want to brush up prior to proceeding with this chapter with the essential background information presented in Appendix A - New User Background Information. *Even if you are a UNIX user and find the tools and files familiar, do not configure this product as you would a regular Linux server.*

The chapter is divided into the following sections:

- **System Requirements**
- **Default Configuration Parameters**
- **Pre-Install Checklist**
- **Task List**
- **The Wizard**
- **Quick Start**
- **The Installation and Configuration Process**

**System Requirements**

Cyclades recommends either of the following specifications for configuration of the Cyclades-TS:

- A workstation with a console serial port, or
- A workstation with Ethernet and TCP/IP topology
The following table shows the different hardware required for various configuration methods:

<table>
<thead>
<tr>
<th>Hardware</th>
<th>Configuration Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Console, Console Cable (constructed from RJ-45 straight-through cable + adapter)</td>
<td>vi, Wizard, or CLI</td>
</tr>
<tr>
<td>Workstation, Hub, Ethernet Cables</td>
<td>vi, Wizard, CLI, or browser</td>
</tr>
</tbody>
</table>

If you will be using vi, the files that need to be changed are discussed in Configuration using Telnet in this chapter. If you will be using the Wizard, basic Wizard access can be found under Configuration Wizard - Basic Wizard in Chapter 3 - Additional Features and specifics of this method are discussed under the appropriate option title in the same chapter. If you choose the browser method, the Quick Start in this chapter shows the screen flow and input values needed for this configuration mode. If you choose the CLI (Command Line Interface) method, this allows you to configure certain parameters for a specified serial port or some network-related parameters. Specifics of this method are discussed under the appropriate option title in Chapter 3 - Additional Features.

**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

There are several things you will need to confirm prior to installing and configuring the Cyclades-TS:

| **Root Access** | You will need Root Access on your local UNIX machine in order to use the serial port. |
| **HyperTerminal, Kermit, or Minicom** | If you are using a PC, you will need to ensure that HyperTerminal is set up on your Windows operating system. If you have a UNIX operating system, you will be using Kermit or Minicom. |
| **IP Address of:** | You will need to locate the IP address of your PC or workstation, the Cyclades-TS, and the machine that resolves names on your network. Your Network Administrator can supply you with these. |
| **PC or terminal,** | If there is outside access to the LAN that the Cyclades-TS will be connected with, you will need the gateway IP address as well. |
| **Cyclades-TS,** | |
| **NameServer, and Gateway** | |
| **Network Access** | You will need to have a NIC card installed in your PC to provide an Ethernet port, and have network access. |
Chapter 2 - Installation, Configuration, Usage

Task List

There are eight key tasks that you will need to perform to install and configure the Cyclades-TS:

Task 1: Connect the Cyclades-TS to the Network and other Devices.
Task 2: Configure the COM Port Connection and Log In.
Task 3: Modify the System Files.
Task 4: Edit the pslave.conf file.
Task 5: Activate the changes.
Task 6: Test the configuration.
Task 7: Save the changes.
Task 8: Reboot the Cyclades-TS

The Wizard

The eight key tasks can also be done through a wizard in the 1.3.4 plus versions of the Cyclades-TS.

Basic Wizard
The Basic Wizard will configure the following parameters:

- Hostname
- DHCP enabled/disabled
- System IP (if DHCP is disabled)
- Netmask (if DHCP is disabled)
- Default Gateway
- DNS Server
- Domain
Basic Wizard access is covered in the Quick Start in this chapter and also in Configuration Wizard - Basic Wizard in Chapter 3 - Additional Features.

Custom Wizard

Further configuration of the Cyclades-TS can be done through one of several customized wizards. These procedures are explained under their respective topic heading in Chapter 3 - Additional Features. There are custom wizards for the following optional configurations:

- **Access Method**
- **Generating Alarms**
- **Authentication**
- **Data Buffering**
- **Help**
- **Power Management**
- **Serial Settings**
- **Session Sniffing**
- **Syslog**
- **Terminal Appearance**
- **TS Setup Wizard** (These are additional configuration parameters applied only to the TS profile.)

**Important!** If you are installing and configuring the Cyclades-TS110/100, there are special requirements and instructions. Be sure to read Special Configuration for the Cyclades-TS110/100 at the end of this chapter.
Chapter 2 - Installation, Configuration, Usage

Quick Start

This Quick Start gives you all the necessary information to quickly configure and start using the Cyclades-TS as a Console Access Server (CAS). The complete version of this process is listed later in this chapter under The Installation and Configuration Process. New Users may wish to follow the latter instruction set, as this Quick Start does not contain a lot of assumed knowledge.

You can configure the Cyclades-TS by any one of four methods:

- Console
- Browser
- Telnet
- CLI (Command Line Interface)

If you have a serial port that you can use as a console port, use the Console method. If you have access to telnet, you can use this method, while New Users may prefer the Browser method for its user-friendliness.

**Important!** Take care when changing the IP address of the Cyclades-TS. Confirm the address you are changing it to. (You may want to write it down.)

Configuration using a Console

**Step 1: Connect the console cable.**

Connect the console cable (created from the RJ-45 straight-through cable and the appropriate console adapter) to the port labeled “Console” on the Cyclades-TS with the RJ-45 connector end, and to your PC’s available COM port with the serial port end.
Step 2: Power on the Cyclades-TS.
After the Cyclades-TS finishes booting, you will see a login prompt on the console screen.

Step 3: Enter root as login name and tslinux as password.

Step 4: Type wiz and press Enter.
A configuration wizard screen will appear in your Hyperterminal session, asking you a series of questions.

***********************************************************
*********** 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...

You will want to configure the following settings:

- Hostname
- DHCP enabled/disabled
- System IP (if DHCP is disabled)
- Domain Name
- Primary DNS Server
Chapter 2 - Installation, Configuration, Usage

- Gateway IP
- Network Mask (if DHCP is disabled)

After you input the requested parameters you will receive a confirmation screen:

Current configuration:

Hostname : CAS
DHCP : enabled
Domain name : cyclades.com
Primary DNS Server : 197.168.160.200
Gateway IP : 192.168.160.1

If the parameters are correct, "y" should be typed; otherwise, type "n" and then "c" when asked to change the parameters or quit the program. After the parameters are confirmed, the next question will be whether to save the configuration to flash. Select "y" to make the new configuration permanent in non-volatile memory.

After you confirm and save the basic parameters, you will be presented with the shell prompt. From there, either select to continue configuration using the vi editor or use the browser or CLI method (if appropriate).

The Cyclades-TS is now configured as a CAS with its new IP address, with no authentication, and accepting telnet to the serial ports. You can telnet the CAS IP + serial port 1 with the following command:

telnet <IP assigned by DHCP Server or by you> 7001

Note. Serial port 1 is configured as 9600, 8N1 by default. The server connected to this serial port has to have the same configuration for its serial port.

To explore the Cyclades-TS features, either continue configuration using the vi editor from the console or use a browser from a workstation and point to the Cyclades-TS.
Chapter 2 - Installation, Configuration, Usage

Configuration using a Web browser

The Cyclades-TS box comes with DHCP client enabled. If you have a DHCP Server installed on your LAN, you can skip Step 2 below. If not, the DHCP request will fail and an IP address pre-configured on the Console server's Ethernet interface (192.168.160.10) will be used instead. To access the box using your browser:

Step 1: Connect Hub to workstation and TS.
Your workstation and your TS must be on the same physical LAN. Connect one RJ-45 cable from the Ethernet port of the TS to a spare port from a hub, and another cable from another spare port of that same hub to the workstation used to manage the servers.

Step 2: If you do not have a DHCP Server in your LAN, add a route pointing to the TS IP.
From the workstation, issue a command to add a route pointing to the network IP address of the TS (192.168.160.0) accessed through the workstation’s Ethernet interface.

For Linux, the command would be:

```
route add -net 192.168.160.0/24 gw <IP address assigned to the workstation’s Ethernet interface>
```

Example: if the workstation has IP address 200.246.93.150 the command would be:

```
route add -net 192.168.160.0/24 gw 200.246.93.150
```

For Windows, the command would be:

```
route add 192.168.160.0 mask 255.255.255.0 <IP address assigned to the workstation’s Ethernet interface>
```

Example: if the workstation has IP address 200.246.93.150 the command would be:

```
route add 192.168.160.0 mask 255.255.255.0 200.246.93.150
```

Step 3: Point your browser to the IP address assigned by the DHCP Server (or to 192.168.160.10 if there is no DHCP Server in your LAN).
The login page shown in the following figure will appear.
Step 4: Enter *root* as login name and *tslinux* as password.

Step 5: Click the Submit button.

This will take you to the Configuration & Administration Menu page, shown in the following figure:
This page gives a brief description of all menu options. A menu of links is provided along the left side of the page. A summary of what each link leads to is shown on Table 3: Configuration Section through Table 6: Information Section.

Security Issue. Change the password of the Web root user as soon as possible. The user database for the Web Configuration Manager is different than the system user database, so the root password can be different. See Changing the Root Password in Appendix F - Web User Management.

Step 6: Click on the General link.
Step 7: Configure parameters presented in the fields.

Step 8: Click on the Submit button.
Make the changes effective.
Click on the Administration > Run Configuration link, check the Serial Ports/Ethernet/Static Routes box and click on the Activate Configuration button.
If you disabled DHCP and changed your Ethernet IP, you will lose your connection. You will need to use your browser to connect to the new IP.

Step 9: Click on the Save Configuration to Flash button.
The configuration was saved in flash. The new configuration will be valid and running. The Cyclades-TS is now configured as a CAS with its assigned (by DHCP Server or you) IP address, with no authentication, and accepting telnet to the serial ports. You can telnet the CAS IP + serial port 1 with the following command:

telnet <IP assigned> 7001
To explore the Cyclades-TS features, either continue configuration using your browser, use the vi editor from the console, or use CLI, if appropriate.

A description of each of the links on the five sections of the Configuration and Administration menu page is provided on the following five tables:

### Table 2: Applications Section

<table>
<thead>
<tr>
<th>Link Name</th>
<th>Description of Page Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logout</td>
<td>Exits the Web Management Service</td>
</tr>
<tr>
<td>Connect to Serial Ports</td>
<td>Telnet/SSH connection to Portslave</td>
</tr>
<tr>
<td>Link Name</td>
<td>Description of Page Contents</td>
</tr>
<tr>
<td>----------------</td>
<td>---------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Configuration</td>
<td>This section contains the configuration tools</td>
</tr>
<tr>
<td>General</td>
<td>Unit Description, Ethernet, DNS, Name Service Access, Data Buffering</td>
</tr>
<tr>
<td>Syslog</td>
<td>Configuration for the syslog-ng</td>
</tr>
<tr>
<td>SNMP</td>
<td>Configuration for the SNMP server</td>
</tr>
<tr>
<td>Serial Ports</td>
<td>Configuration of Portslave package</td>
</tr>
<tr>
<td>Serial Port Groups</td>
<td>Configuration of User Groups for Serial Ports</td>
</tr>
<tr>
<td>Host Table</td>
<td>Table of hosts in /etc/hosts</td>
</tr>
<tr>
<td>Static Routes</td>
<td>Static routes defined in /etc/network/st_routes</td>
</tr>
<tr>
<td>IP Chains</td>
<td>Shows IP Chains entries</td>
</tr>
<tr>
<td>Boot Configuration</td>
<td>Configuration of parameters used in the boot process</td>
</tr>
<tr>
<td>Edit Text File</td>
<td>Tool to edit a configuration file</td>
</tr>
<tr>
<td>System Users</td>
<td>Management of system users defined in /etc/password</td>
</tr>
<tr>
<td>System Groups</td>
<td>Management of system groups defined in /etc/groups</td>
</tr>
</tbody>
</table>
## Chapter 2 - Installation, Configuration, Usage

### Table 4: Administration Section

<table>
<thead>
<tr>
<th>Link Name</th>
<th>Description of Page Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Reboot</strong></td>
<td>Resets the equipment</td>
</tr>
<tr>
<td><strong>Download/Upload Image</strong></td>
<td>Uses an FTP server to load/save a kernel image</td>
</tr>
<tr>
<td><strong>Load/Save Configuration</strong></td>
<td>Uses flash memory or an FTP server to load or save the TS' configuration</td>
</tr>
<tr>
<td><strong>Run Configuration</strong></td>
<td>Makes the configuration changes effective</td>
</tr>
<tr>
<td><strong>Set Date/Time</strong></td>
<td>Set the TS’ date and time</td>
</tr>
<tr>
<td><strong>Active Sessions</strong></td>
<td>Shows the active sessions</td>
</tr>
<tr>
<td><strong>Process Status</strong></td>
<td>Shows the running processes and allows the administrator to kill them</td>
</tr>
<tr>
<td><strong>Restart Processes</strong></td>
<td>Allows the administrator to start or stop some specific processes</td>
</tr>
<tr>
<td><strong>PCMCIA</strong></td>
<td>Allows the administrator to insert and eject PCMCIA cards</td>
</tr>
</tbody>
</table>

### Table 5: Web User Management Section

<table>
<thead>
<tr>
<th>Link Name</th>
<th>Description of Page Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Users</strong></td>
<td>List of users allowed to access the Web server</td>
</tr>
<tr>
<td><strong>Groups</strong></td>
<td>List of possible access groups</td>
</tr>
<tr>
<td><strong>Access Limits</strong></td>
<td>List of access limits for specific URLs</td>
</tr>
<tr>
<td><strong>Load/Save Configuration</strong></td>
<td>Load/Save Configuration in /etc/websum.conf</td>
</tr>
</tbody>
</table>
## Table 6: Information Section

<table>
<thead>
<tr>
<th>Link Name</th>
<th>Description of Page Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Interface Statistics</strong></td>
<td>Shows statistics for all active interfaces</td>
</tr>
<tr>
<td><strong>DHCP client</strong></td>
<td>Shows host information from DHCP</td>
</tr>
<tr>
<td><strong>Serial Ports</strong></td>
<td>Shows the status of all serial ports</td>
</tr>
<tr>
<td><strong>Routing Table</strong></td>
<td>Shows the routing table and allows the administrator to add or delete routes</td>
</tr>
<tr>
<td><strong>ARP Cache</strong></td>
<td>Shows the ARP cache</td>
</tr>
<tr>
<td><strong>IP Statistics</strong></td>
<td>Shows IP protocol statistics</td>
</tr>
<tr>
<td><strong>ICMP Statistics</strong></td>
<td>Shows ICMP protocol statistics</td>
</tr>
<tr>
<td><strong>TCP Statistics</strong></td>
<td>Shows TCP protocol statistics</td>
</tr>
<tr>
<td><strong>UDP Statistics</strong></td>
<td>Shows UDP protocol statistics</td>
</tr>
<tr>
<td><strong>RAM Disk Usage</strong></td>
<td>Shows the TS File System status</td>
</tr>
<tr>
<td><strong>System Information</strong></td>
<td>Shows information about the kernel, time, CPU, and memory</td>
</tr>
</tbody>
</table>
Chapter 2 - Installation, Configuration, Usage

Configuration using Telnet

The Cyclades-TS box comes with DHCP client enabled. If you have a DHCP Server installed on your LAN, you can skip Step 2 below. If not, the DHCP request will fail and an IP address pre-configured on the Console server's Ethernet interface (192.168.160.10) will be used instead. To access the box using telnet:

Step 1: **Connect Hub to workstation and TS.**
Your workstation and your TS must be on the same physical LAN. Connect one RJ-45 cable from the Ethernet port of the TS to a spare port from a hub, and another cable from another spare port of that same hub to the workstation used to manage the servers.

Step 2: **If you do not have a DHCP Server in your LAN, add a route pointing to the TS IP.**
From the workstation issue a command to add a route pointing to the network IP address of the TS (192.168.160.0) accessed through the workstation’s Ethernet interface.

For Linux, the command would be:

```
route add -net 192.168.160.0/24 gw <IP address assigned to the workstation’s Ethernet interface>
```

Example: if the workstation has IP address 200.246.93.150 the command would be:

```
route add -net 192.168.160.0/24 gw 200.246.93.150
```

For Windows, the command would be:

```
route add 192.168.160.0 mask 255.255.255.0 <IP address assigned to the workstation’s Ethernet interface>
```

Example: if the workstation has IP address 200.246.93.150 the command would be:

```
route add 192.168.160.0 mask 255.255.255.0 200.246.93.150
```

Step 3: **Telnet to <IP assigned by DHCP Server or 192.168.160.10 if there is no DHCP Server>.**

Step 4: **Enter root as login name and tslinux as password.**
Step 5: Type `wiz` and press Enter.

A Configuration Wizard screen will appear on your telnet screen, asking you a series of questions.

***********************************************************
********* CONFIGURATION WIZARD ***********
***********************************************************

INSTRUCTIONS for using the Wizard:
You can:
1) Enter the appropriate information for your system and press ENTER. Enter '#' if you want to deactivate that parameter 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...

After you input the requested parameters you will receive a confirmation screen:

Current configuration:
Hostname : CAS
DHCP: disabled
System IP : 192.168.160.10
Domain name : cyclades.com
Primary DNS Server : 197.168.160.200
Gateway : eth0
Network Mask : 255.255.255.0
If the parameters are correct, “y” should be typed; otherwise, type “n” and then “c” when asked to change the parameters or quit the program. After the parameters are confirmed, the next question will be whether to save the configuration to flash. Select “y” to make the new configuration permanent in non-volatile memory.

At this point you may lose your connection when saving the changes, if you disabled DHCP and assigned an IP address. Don’t worry! The new configuration will be valid. The Cyclades-TS is now configured as a CAS with its assigned (by DHCP or you) IP address, with no authentication, and accepting telnet to the serial ports. You can telnet the CAS IP + serial port 1 with the following command:

telnet <IP assigned> 7001

Note. Serial port 1 is configured as 9600, 8N1 by default. The server connected to this serial port has to have the same configuration for its serial port.

After you confirm the basic parameters, you will be presented with the shell prompt. From there, either select to continue configuration using the vi editor or continue using a browser. For additional configuration, see Chapter 3 - Additional Features in this guide.
Chapter 2 - Installation, Configuration, Usage

The Installation and Configuration Process

Task 1: Connect the Cyclades-TS to the Network and other Devices

Power Users

Connect a PC or terminal to the Cyclades-TS using the console cable. If you are using a PC, HyperTerminal can be used in the Windows operating system and Kermit or Minicom in the UNIX operating system. When the Cyclades-TS boots properly, a login banner will appear. Log in as root (default password is tslinux). A new password should be created as soon as possible. The terminal parameters should be set as follows:

- Serial Speed: 9600 bps
- Data Length: 8 bits
- Parity: None
- Stop Bits: 1 stop bit
- Flow Control: none
- ANSI emulation

You may now skip to Task 4: Edit the pslave.conf file.

**Important!** Any configuration change must be saved in flash once validated. To save in Flash run saveconf (see Task 7: Save the changes). To validate/activate a configuration, run signal_ras bup (see Task 5: Activate the changes).

**Note:** If your terminal does not have ANSI emulation, select vt100; then, on the TS, log in as root and switch to vt100 by typing:

TERM=vt100;export TERM
Chapter 2 - Installation, Configuration, Usage

**Tip.** We strongly recommend to use 9600 bps console speed. In case you need to use another speed please check Appendix D - Software Upgrades and Troubleshooting.

**Important!** Always complete ALL the steps for your chosen configuration before testing or switching to another configuration.

New Users

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

After the initial configuration through the HyperTerminal connection, you will be connecting your PC (or another terminal) to the Cyclades-TS via an Ethernet connection in order to manage the TS. The workstation used to access the TS through telnet or ssh uses a LAN connection.

These events can be summarized as follows:

- PC (Hyper terminal): COM port connects via serial cable to the TS’s console port.
- PC (Ethernet): Ethernet port connects via hub to the TS’s Ethernet port.
- Use the HyperTerminal to configure the box.
- Use the PC Ethernet to access the box as client (telnet/ssh).
Chapter 2 - Installation, Configuration, Usage

Step 1: Plug the power cable into the Cyclades-TS.
Insert the female end of the black power cable into the power socket on the Cyclades-TS and the three-prong end into a wall outlet.

DANGER! To help prevent electric shock, plug the Cyclades-TS 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. For the TS110/100, 400, and 800, the grounded power cable constraint does not apply, as these products have an external power supply, and one power cable instead of two.

Step 2: Connect the console cable.
You will be constructing a Console Cable out of the RJ-45 straight-through cable and the appropriate adapter provided in the product box. (There are four options: 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 Cyclades-TS with the RJ-45 connector end, and connect the adapter end to your PC’s available COM port. For more detailed information on cables, see Appendix B - Cabling, Hardware, and Electrical Specifications.

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

Step 3: Connect Hub to PC and the Cyclades-TS.
Your workstation and TS must be on the same physical LAN. Connect one RJ-45 cable from the Ethernet port of the TS to the hub, and another from the hub to the workstation used to manage the servers.

Step 4: Install and launch HyperTerminal, Kermit or Minicom if not already installed.
You can obtain the latest update to HyperTerminal from:

http://www.hilgraeve.com/htpe/download.html
Chapter 2 - Installation, Configuration, Usage

Task 2: Configure the COM Port Connection and Log In

Step 1: Select available COM port.

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

![Figure 13: Choose a free COM port](image)

Step 2: Configure COM port.

Click the Configure button (hidden by the dropdown menu in the above figure). Your PC, considered here to be a “dumb terminal,” should be configured to use 9600 bps, 8 data bits, no parity, 1 stop bit, and no flow control (as shown in the following figure).
Step 3: **Power on the Cyclades-TS.**

Step 4: **Click OK on the Properties window.**

You will see the Cyclades-TS booting on your screen. After it finishes booting, you will see a login prompt.
Task 3: Modify the System Files

When the Cyclades-TS finishes booting, a prompt will appear (a flashing underline cursor) in your HyperTerminal window. You will modify the following Linux files to let the Cyclades-TS know about its local environment:

/etc/hostname
/etc/hosts
/etc/resolv.conf
/etc/network/st_routes
/etc/inittab (Cyclades-TS110/100 only)

Important! If you have the Cyclades-TS110/100 you will be modifying an additional file: /etc/inittab. See Configuring the Cyclades-TS110/100 for the first time at the end of this chapter for instructions specific to this model.

The five Linux files must be modified to identify the TS and other devices it will be communicating with. The operating system provides the vi editor, which is described in Appendix A - New User Background Information for the uninitiated. The Cyclades-TS runs Linux, a UNIX-like operating system, and those not familiar with it will want to refer to Appendix A.

Step 1: Type root and press Enter.

Step 2: At the password prompt, type tslinux.
Press Enter.

Step 3: Modify /etc/hostname.

In HyperTerminal, type “vi /etc/hostname” (without the quotes) and press Enter. Arrow over the existing text in the file, type “r” (for replace) and type the first number of the model of your Cyclades-TS. (Or, you can replace the default naming convention with anything you’d like for your hostname.) When finished, press the Esc key, (to return to command mode), then type “:” (colon), and then “wq” and press Enter. This will save the file. (The only entry in this file should be the hostname of the Cyclades-TS.) An example is shown in the following figure. (The
HyperTerminal screen is shown in this first example for clarity, however, for the other Linux files we will modify, only the command line text will be shown.

**Figure 15: The /etc/hostname file with hostname typed in**

**Step 4: Modify /etc/hosts.**

This file should contain the IP address for the Ethernet interface and the same hostname that you entered in the /etc/hostname file. It may also contain IP addresses and host names for other hosts in the network. Modify the file using the vi as you did in Step 1.

**Figure 16: Contents of the /etc/hosts file**

**Step 5: Modify /etc/resolv.conf.**

This file must contain the domain name and nameserver information for the network. Obtain the nameserver IP address from your Network Administrator. The default contents of this file are:

```plaintext
domain mycompany.com
nameserver 200.200.200.2
```
**Chapter 2 - Installation, Configuration, Usage**

**Step 6: Modify `/etc/network/st_routes`**.

The fourth file defines static routes. In the console server example in [Figure 62: Console Access Server diagram](#) the router is a gateway router and thus its IP address is configured in this file to be the default gateway. Other static routes are also configured in this file. If you will be managing servers through a LAN, you don’t need to alter this file. If you will be managing via Internet, you will be connecting through a router, and thus need to modify this file. You would get the IP address from your Network Administrator. The default contents of this file are:

```
route add default dev eth0
```

**Step 7: Change password for root and new users.**

The default `/etc/passwd` file has the user “root” with password “tslinux”. You should change the password for user root as soon as possible. Before changing any password or adding new users you should also activate shadow password, if it is needed. The Cyclades-TS has support for shadow password, but it is not active by default. To activate shadow password follow the steps listed below:

**Step A: Create an empty file called `/etc/shadow`.**

```
# touch /etc/shadow
```

**Step B: Add a temporary user to the system. It will be removed later.**

```
# adduser boo
```

**Step C: Edit the file `/etc/shadow`.**

For each user in passwd file, create a copy of the line that begins with “boo:" in the shadow file, then replace “boo” with the user name. The line beginning with “root” must be the first line in the file `/etc/shadow`. The following lines show how the `/etc/shadow` file should be.

```
root:EreFjH95c1x6Y:12408:0:99999:7:-1:-1:
rpc:EreFjH95c1x6Y:12408:0:99999:7:-1:-1:
nobody:EreFjH95c1x6Y:12408:0:99999:7:-1:-1:
sshd:EreFjH95c1x6Y:12408:0:99999:7:-1:-1:
boo:EreFjH95c1x6Y:12408:0:99999:7:-1:-1:
```

**Step D: Edit the `passwd` file.**

Replace the password in all password fields with an “x”. The root’s line will look like this:
Chapter 2 - Installation, Configuration, Usage

“root:x:0:0:root:/root:/bin/sh”
^ password field

The /etc/passwd file should look like this:

root:x:0:0:root:/root:/bin/sh
rpc:x:1:1:Portmapper RPC user:/:/bin/false
nobody:x:99:99:Nobody:/:
sshd:x:501:501:sshd privsep:/var/empty:/bin/false
boo:x:505:505:Embedix User,,,:/home/boo:/bin/sh

Tip. Using the vi editor, put the cursor in the first byte after “root:”, then type “ct:x” plus <ESC>.

Step E: Remove the temporary user boo.
# deluser boo

Step F: Change the password for all users and add the new ones needed.
# passwd <username>
or
# adduser <username>

Step G: Edit /etc/config_files and add a line with “/etc/shadow.”

Task 4: Edit the pslave.conf file

This is the main configuration file (/etc/portslave/pslave.conf) that contains most product parameters and defines the functionality of the Cyclades-TS. Only three parameters need to be modified or confirmed for a basic configuration:

- conf.eth_ip (if you disabled DHCP)
- all.authtype
- all.protocol
A listing of the pslave.conf file with all possible parameters, as well as the files used to create other configurations from parameters in this file, is provided in Appendix C - The pslave Configuration File. Additional, optional modifications made to this file will depend on the configuration desired.

There are three basic types of parameters in this file:

- `conf.*` parameters are global or apply to the Ethernet interface.
- `all.*` parameters are used to set default parameters for all ports.
- `s#.*` parameters change the default port parameters for individual ports.

An all.* parameter can be overridden by a s#.* parameter appearing later in the pslave.conf file (or vice-versa).

**Power Users:** To find out what to input for these three parameters so that you can configure what you need, go the appropriate appendix, where you will find a complete table with an explanation for each parameter. You can use the templates from that same Appendix (pslave.conf.cas, etc.) as reference.

**conf.eth_ip** This is the IP address of the Ethernet interface. Use it if you don’t have DHCP Server in your LAN. An example value would be:

200.200.200.1
This parameter controls the authentication required by the Cyclades-TS. The authentication required by the device to which the user is connecting is controlled separately. There are several authentication type options:

- **none** (no authentication)
- **local** (authentication is performed using the /etc/passwd file)
- **remote** (This is for a terminal profile only. The unit takes in a username but does not use it for authentication. Instead it passes it to the remote server where it is then used for authentication.)
- **radius** (authentication is performed using a Radius authentication server)
- **TacacsPlus** (authentication is performed using a TacacsPlus authentication server)
- **ldap** (authentication is performed against an ldap database using an ldap server. The IP address and other details of the ldap server are defined in the file /etc/ldap.conf)
- **local/radius** (authentication is performed locally first, switching to Radius if unsuccessful)
- **radius/local** (the opposite of the previous option)
- **local/TacacsPlus** (authentication is performed locally first, switching to TacacsPlus if unsuccessful)
- **TacacsPlus/local** (the opposite of the previous option)
- **TacacsPlusDownLocal** (local authentication is tried only when the TacacsPlus server is down)
- **RadiusDownLocal** (local authentication is tried only when the Radius server is down)
- **ldapDownLocal** (local authentication is tried only when the ldap server is down)
Chapter 2 - Installation, Configuration, Usage

- NIS - All authentication types but NIS follow the format all.authtype <Authentication>DownLocal or <Authentication> (e.g. all.authtype radius or radiusDownLocal or ldap or ldapDownLocal, etc). NIS requires all.authtype to be set as local, regardless if it will be "nis" or its "Downlocal" equivalent. The service related to "nis" or its “Downlocal” equivalent would be configured in the /etc/nsswitch.conf file, not in the /etc/portslave/pslave.conf file.

An example value would be:

```
radius
```

*all.protocol*  For the console server configuration, the possible protocols are:

- `socket_server` (when telnet is used)
- `socket_ssh` (when ssh version one or two is used)
- `raw_data` (to exchange data in transparent mode - similar to `socket_server` mode, but without telnet negotiation, breaks to serial ports, etc.)

An example value would be:

```
socket_server
```

The Authentication feature
See Authentication in Chapter 3 - Additional Features.

**Task 5: Activate the changes**
Execute the following command in HyperTerminal to activate the changes:
```
signal_ras hup
```

**Task 6: Test the configuration**
Now you will want to make sure that the ports have been set up properly.

**Step 1: Ping the TS from a DOS prompt.**
Open a DOS window, type in the following, and then press Enter:
```
ping <IP assigned to the TS by DHCP or you>
```
An example would be:

```
ping 192.168.160.10
```

If you receive a reply, your TS connection is OK. If there is no reply see Appendix D - Software Upgrades and Troubleshooting.

**Step 2: Telnet to the server connected to the first port of the Cyclades-TS.**

(This will only work if you selected socket_server as your all.protocol parameter.)

While still in the DOS window, type the following and then press Enter:

```
telnet <IP assigned to the TS by DHCP or you> 7001
```

An example would be:

```
telnet 192.168.160.10 7001
```

If everything is configured correctly, a telnet session should open on the server connected to port 1. If not, check the configuration, follow the above steps again, and check Appendix D - Software Upgrades and Troubleshooting.

**Task 7: Save the changes**

Execute the following command in HyperTerminal to save the configuration:

```
saveconf
```

**Task 8: Reboot the Cyclades-TS**

After rebooting, the initial configuration is complete.

**Note:** restoreconf does the opposite of saveconf, copying the contents of the /proc/flash/script file to the corresponding files in the ramdisk. The files on the ramdisk are overwritten. Restoreconf is run automatically each time the Cyclades-TS is booted.
Chapter 2 - Installation, Configuration, Usage

Special Configuration for the Cyclades-TS110/100

TS110/100-specific background information

Since there are two configurable physical interfaces available in the TS110/100 (RS-232 and RS-485), these models require the configuration of the parameter described below.

all.media or*
s1.media

(*see note box below)

For the TS110/100 only.

- rs232 (RS-232 interface and DB-9 connector),
- rs485_half_terminator (RS-485 interface, half duplex communication with two wires, DB-9 or Terminal Block. The TS110/100 terminates the network),
- rs422 (RS-485 interface, full duplex communication with four wires, DB-9 or Terminal Block. The TS110/100 terminates the network), or
- rs485_half (RS485 interface, half duplex communication with two wires, DB-9 or Terminal Block. The TS110/100 is in the middle of the network.)

Note: Note: all.* parameters are used to set default parameters for all ports and s#.* parameters change the default parameters for individual ports. As the TS110/100 has only one port, either s1* or all.* can be used interchangeably.
DANGER! When reconfiguring the media from RS232 to RS485 (or RS485 to RS232), it is extremely important to remove the serial cable (DB9 connector) before issuing signal_ras hup or signal_ras start (to make valid the new configuration). Using wrong cable for that newly configured media may burn the serial interface.

When using Web or telnet/ssh session to reconfigure the media, follow these steps:
1) Remove the serial cable before the reconfiguration
2) Start the reconfiguration process
3) Save and submit the changes (e.g. signal_ras hup)
4) Insert the new serial cable compatible with the new media

When using console for the configuration, follow these steps:
1) Edit the proper configuration file
2) Quit editor, saving the changes
3) Run saveconf
4) Remove the serial cable
5) Power the unit off
6) Insert the new serial cable compatible with the new media
7) Power the unit back on

Configuring the Cyclades-TS110/100 for the first time

The Cyclades-TS110/100 does not have a dedicated console port. Therefore, after configuring the serial port, perform the following steps:
Chapter 2 - Installation, Configuration, Usage

Step 1: Edit the file /etc/inittab.
Comment the line that designates the console port (add a "#" to it):

```
# ttyS0::respawn:/sbin/getty -p ttyS0 ansi
```

Uncommenting the line starts the program cy_buffering (remove the '#' from the beginning):

```
::once:/sbin/cy_buffering
```

Step 2: Run saveconf.
The command saveconf, which reads the /etc/config_files file, should be run. The command saveconf copies all the files listed in the file /etc/config_files from the ramdisk to /proc/flash/script. The previous contents of the file /proc/flash/script will be lost.

Step 3: Reboot.
After rebooting the TS110/100, the initial configuration is complete.
Chapter 2 - Installation, Configuration, Usage

Accessing the Serial Ports

There are four ways to access the serial ports, depending on the protocol you configured for that serial port (all.protocol being socket_server for telnet access, socket_ssh for ssh access, etc).

Opening and closing a telnet session to a serial port

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

telnet <CAS hostname> <TCP port number>

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

Note: restoreconf does the opposite of saveconf, copying the contents of the /proc/flash/script file to the corresponding files in the ramdisk. The files on the ramdisk are overwritten. Restoreconf is run automatically each time the Cyclades-TS is booted.

<TCP port number> is the number associated to the serial port. From factory, 7001 corresponds to serial port 1, 7002 to serial port 2 and so forth.

To close the telnet session, just press the telnet hot key configured in telnet client application (usually it's "Ctrl J") and "q" to quit.

Opening and closing an SSH session to a serial port

To open an ssh session to a serial port, issue the command:

ssh -l <Username>:@<Server> <CAS hostname>

<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, etc database.

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

<CAS hostname> 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 Cyclades-TS (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 ".~").

Accessing Serial Ports using “ts_menu”

To access the serial port (telnet or ssh) using ts_menu, login to the CAS unit and, after receiving the shell prompt, run ts_menu. The servers (aliases) or serial ports will be shown as option to start a connection (telnet/ssh). After typing ts_menu, you will see something similar to the following:

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:

How to close the session from ts_menu (from the console of your unit)

Step 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 ^]

After entering the escape character, the following 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

Step 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.
How to close the session from ts_menu (from a telnet session to your unit)

You have to be sure that a different escape character is used for exiting your telnet/SSH ses-

sion; 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/SSH to your
unit, use the -e option. So for example, to set Ctrl-? as the escape character, type:

telnet -e ^? 192.168.160.10

ssh -e ^? user1@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. To exit from
the entire SSH session to your unit, type the escape character you had set plus character
"."(dot)
Chapter 3 - Additional Features

Introduction

After the Configuration Wizard section in this chapter, each of the following sections is listed alphabetically and shows how to configure the option using vi, the custom Wizard (when available), browser, where appropriate, and the Command Line Interface (CLI), when available. This chapter contains the following sections:

- Configuration Wizard - Basic Wizard
- Access Method
- Authentication
- CAS Port Pool
- Centralized Management
- Clustering
- CronD
- Data Buffering
- DHCP
- Filters
- Generating Alarms
- Help
- Modbus
- NTP
- Ports Configured as Terminal Servers
- Serial Settings
- Session Sniffing
- SNMP
- Syslog
The configuration wizard application is a quicker and easier way to configure the Cyclades-TS. It is recommended that you use this application if you are not familiar with the vi editor or if you just want to do a quick installation of the TS.

The command `wiz` gets you started with some basic configuration. After executing this command, you can continue the configuration of the TS using any browser or by editing system files with the vi editor. What follows are the basic parameters to get you quickly started. The files that will be eventually modified if you decide to save to flash at the end of this application are:

1. `/etc/hostname`
2. `/etc/hosts`
3. `/etc/resolv.conf`
4. `/etc/network/st_routes`
5. `/etc/network/ifcfg_eth0`
6. `/etc/portslave/pslave.conf`
Chapter 3 - Additional Features

Step 1: Enter the command *wiz*.

At the command prompt type “wiz” in your terminal to bring up the wizard. You will receive an initial instruction screen.

***********************************************************
********* C O N F I G U R A T I O N    W I Z A R D ***********
***********************************************************

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...

Step 2: Press Enter to continue with the wizard.

You will see the current configurations and have the choice of setting them to default values, or not.

***********************************************************
********* C O N F I G U R A T I O N    W I Z A R D ***********
***********************************************************

Current configuration:

Hostname: CAS
DHCP: enabled
Domain name: #
Primary DNS Server: #
Gateway IP: eth0
Set to defaults? (y/n) [n] :

**Step 3:** **Press Enter or type n or y:**

The default answer or value to any question is in the brackets. You can take one of three actions:

- Either just press the ENTER key to execute whatever is in between the brackets, or
- Type n to NOT reset the current configurations to the Cyclades defaults, or
- Type y to reset to Cyclades default configurations.

---

**Tip.** On most of the following configuration screens, the default or current value of the parameter is displayed inside brackets. Just press the ENTER key if you are satisfied with the value in the brackets. If not, enter the appropriate parameter and press ENTER.

If at any time after choosing whether to set your configurations to default or not, you want to exit the wizard or skip the rest of the configurations, press ESC. This will immediately display a summary of the current configurations for your verification before exiting the application. This will not work if you did not enter a valid choice for the parameter you are currently on.

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.

---

**Step 4:** **Enter Hostname and then press the Enter key.**

This is an alias for your TS that allows you to refer to the TS by this name rather than its IP address. Enter hostname after the prompt:

Hostname [CAS]:
Chapter 3 - Additional Features

Step 5: Type y, n, or press Enter to enable or disable DHCP client.

Type y or press Enter if there is a DHCP Server in your LAN, to have the Dynamic Host Configuration Protocol (DHCP) automatically assign an IP address for your TS. Type n to manually assign an IP address.

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

Note: Typing y omits Steps 6 and Step 10.

Step 6: If DHCP client is disabled, enter IP Address of your TS and then press the Enter key.

If the DHCP client is enabled, skip this step. This question will only appear if DHCP client is disabled. This is the IP address of the TS within your network. See your network administrator to obtain a valid IP address for the TS.

IP of your system[]: 192.168.160.10

Step 7: Enter Domain name and then press Enter.

Domain name locates or identifies your organization within the Internet.

Domain name[#]: cyclades.com

Step 8: Enter IP address of Domain Name Server and press Enter.

At the prompt, enter the IP address of the server that resolves domain names. Your domain name is alphabetical so that it is easier to remember. Every time you see the domain name, it is actually being translated into an IP address by the domain name server. See your network administrator to obtain this IP address for the domain name server.

Domain Name Server[#]: 192.168.160.200

Step 9: Enter Gateway IP address and press Enter.

The Gateway is a node on a network that serves as an entrance point into another network. See your network administrator to find out your organization's gateway address.
Configuration Wizard - Basic Wizard

Gateway IP[eth0]: 192.168.160.1

Step 10: If DHCP client is disabled, enter Netmask and press Enter.
If the DHCP client is enabled, skip this step. This question will appear only if DHCP client is disabled. The Netmask is a string of 0s and 1s that mask or screen out the host part of an IP address so that only the network part of the address remains.

Netmask[#]: 255.255.255.0

Step 11: Review configuration parameters.
You will now have the parameters you just configured displayed back to you. If you entered y in Step 5:

**************************************************************************************
********* C O N F I G U R A T I O N   W I Z A R D **********
**************************************************************************************

Current configuration:

Hostname: CAS
DHCP: enabled
Domain name: cyclades.com
Primary DNS Server: 197.168.160.200
Gateway IP: 192.168.160.1

Are all these parameters correct (Y)es or (N)o [N]:

If you entered n in Step 5:

Current configuration:

Hostname: CAS
DHCP: disabled
System IP: 192.168.160.10
Domain name: cyclades.com
Primary DNS Server: 192.168.160.200
Gateway IP: 192.168.160.1
Network Mask: 255.255.255.0

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

Cyclades-TS
Chapter 3 - Additional Features

Step 12: Type \textit{y}, or \textit{n}, or press Enter.

Type \textit{y} if all parameters are correct. Type \textit{n} or just press ENTER if not all the parameters are correct and you want to go back and redo them.

Step 13: If you typed \textit{n} in Step 11, type \textit{c} or \textit{q}.

As directed by the prompt, type \textit{c} to go back to very beginning of this application to change the parameters. Type \textit{q} to exit.

Step 14: If you typed \textit{y} in Step 11, choose whether to activate your configurations.

\begin{verbatim}
***********************************************************
********* C O N F I G U R A T I O N    W I Z A R D *********
***********************************************************

You can now use the browser to finish your system configurations, but before that, please read below.

(Note: If you are NOT connected to this unit through a console, and you have just reconfigured the IP of this unit, activating the new configurations may cause you to lose connection. In that case, please reconnect to the unit by the new IP address, and manually issue a saveconf to save your configurations to flash.)

Do you want to activate your configurations now? (y/n) [y] :
\end{verbatim}

Step 15: Choose whether to save to flash.

Flash is a type of memory that will maintain the information saved on it even after the Cyclades-TS is turned off. Once it is turned on again, the saved information can be recovered. If \textit{y} is entered, the screen will display an explanation of what saving to flash means:

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.
If you choose to save to flash, your configurations thus far will still be in the memory of the TS even after you reboot it. If you don't save to flash and if you were to reboot the system, all your new configurations will be lost and you will have to reconfigure the TS.

Do you want to save your configurations to flash? (y/n) [n]:

**Step 16:** Type 'y' if you want to save to flash. Type 'n' if you don't want to save to flash.

You can now continue TS configurations using the Web browser by typing in the IP address of the TS.

**Using the Wizard through your Browser**

The Web interface supports wizards for serial ports configuration. The wizard is a useful tool that simplifies configuration of serial ports. The Web interface will access the following wizard files:

- `/etc/portslave/pslave.wiz.cas` (CAS)
- `/etc/portslave/pslave.wiz.ts` (TS)
- `/etc/portslave/pslave.wiz.ras` (Dial-in Access)
- `/etc/portslave/pslave.wiz.auto` (Automation)

The step-by-step process to configuring ports for a specific profile appear in the following sections, and the exact screen flow begins with **Figure 17: Configuration and Administration page**.

To summarize the process, the wizard configuration is started by first selecting the desired port(s) on the Port Selection page (**Figure 18: Port Selection page**), clicking Submit, and then selecting either the CAS, TS, or RAS profile buttons on the subsequent Serial Port Configuration Page (**Figure 19: Serial Port Configuration page**). Change the appropriate parameters, and then click the Submit button on the Serial Port Configuration Page. For most applications, the parameters to be changed are:

For CAS:

- Port Speed
- First RADIUS/TacacsPlus Authentication Server
Chapter 3 - Additional Features

- First Accounting Server
- RADIUS/TacacsPlus secret
- Protocol (if the protocol is Socket SSH, Socket Telnet, or Socket Raw)
- Socket Port (keep the “Incremented” option on)

For TS:
- Port Speed
- First RADIUS/TacacsPlus Authentication Server
- First Accounting Server
- RADIUS/TacacsPlus secret
- Protocol (if the protocol is Login, Rlogin, SSH, or Socket Client)
- Socket Port (write the TCP port for the protocol selected; keep the “incremented” option off)

For Dial-in access:
- First RADIUS/TacacsPlus Authentication Server
- First Accounting Server
- RADIUS/TacacsPlus secret
- Remote IP Address (keep the “Incremented” option on)
Access method is how a user accesses a server connected to one of the serial ports on the Cyclades-TS (CAS profile) or how a user connected to one of the serial ports accesses a server in the network (TS profile or Dial-In profile).

Configuration for CAS

Parameters Involved and Passed Values
The parameters involved in configuring Access Method for CAS are as follows:

- **all.ipno**: This is the default IP address of the Cyclades-TS’s serial ports. Any host can access a port using its IP address as long as a path to the address exists in the host’s routing table. An example value would be 192.168.1.101+. The “+” indicates that the first port should be addressed as 192.168.1.101 and the following ports should have consecutive values.

- **all.socket_port**: In the CAS profile, this defines an alternative labeling system for the Cyclades-TS ports. An example value would be 7001+. The “+” after the numerical value causes the serial interfaces to be numbered consecutively. In this example, serial interface 1 is assigned the port value 7001, serial interface 2 is assigned the port value 7002, etc. One example on how this could be used is in the case of all.protocol or s<n>.protocol socket_ssh and the port value (7001, 7002, etc), if supplied by the ssh client like username:port value, the ssh client will be directly connected with the serial interface.

- **all.protocol**: The possible protocols are telnet, ssh1/ssh2 or raw data:
  - `socket_server` = telnet protocol,
  - `socket_ssh` = ssh1/ssh2 protocol,
  - `raw_data` = used to exchange data in transparent mode. Raw_data is similar to socket_server mode but without telnet negotiation breaks to serial ports.
  
  An example value would be `socket_server`. 


**Chapter 3 - Additional Features**

**all.users**
Restricts access to ports by user name (only the users listed can access the port or, using the character “!”, all but the users listed can access the port.) A single comma and spaces/tabs may be used between names. A comma may not appear between the “!” and the first user name. The users may be local, Radius or TacacsPlus. User groups (defined with the parameter conf.group) can be used in combination with user names in the parameter list. Notice that these are common users, not administrators. Example: all.users ! joe, mark, user_group. In this example, the users joe, mark, and members of user_group cannot access the port.

**all.poll_interval**
Valid only for protocols socket_server and raw_data. When not set to zero, this parameter sets the wait for a TCP connection keep-alive timer. If no traffic passes through the Cyclades-TS for this period of time, the Cyclades-TS will send a line status message to the remote device to see if the connection is still up. If not configured, 1000 ms is assumed (the unit for this parameter is ms). If set to zero, line status messages will not be sent to the socket client.

**all.tx_interval**
Valid for protocols socket_server and raw_data. Defines the delay (in milliseconds) before transmission to the Ethernet of data received through a serial port. If not configured, 100ms is assumed. If set to zero or a value above 1000, no buffering will take place.

**all.idletimeout**
Valid only for the CAS configuration (protocols socket_server, socket_ssh, raw_data) and modbus. Specifies how long (in minutes) a connection can remain inactive before it is cut off. If set to zero (the default), the connection will not time out.

**conf.group**
Used to group users to simplify configuration of the parameter all.users later on. This parameter can be used to define more than one group. The format is:

<group name>:<user1>{,<user2>[,<user3>]]

Example: conf.group group_name: user1, user2.

**s<n>.serverfarm**
Alias name given to the server connected to the serial port.
Server_connected.
Example: s1.serverfarm Server_connected_serial1.
vi Method
The parameters described above must be changed by directly editing the /etc/portslave/plsave.conf file.

Browser Method
To configure Access Method with your browser:

**Step 1: Point your browser to the Console Server.**
In the address or location field of your browser type the Console Access Server's IP address. For example:

```
http://10.0.0.0
```

**Step 2: Log in as root and type the Web root password configured by the Web server.**
This will take you to the Configuration and Administration page.

**Step 3: Select the Serial Ports link.**
Click on the Serial Ports link on the Link Panel to the left of the page or in the Configuration section of the page. This will take you to the Port Selection page.
Chapter 3 - Additional Features

Step 4: Select port(s).

On the Port Selection page, choose all ports or an individual port from the dropdown menu. This will take you to the Serial Port Configuration page.
Step 5: **Click the CAS profile button.**
Click the CAS profile button in the wizards section. The default CAS profile parameters are now loaded.

Step 6: **Scroll down to the Profile section.**
You can change the settings for *all.ipno, all.socket_port, and all.protocol* in this section.

![Profile Table](image)

*Figure 20: Profile Section of Serial Port Configuration page*

Step 7: **Scroll to the Authentication Section.**
You can configure the parameter *all.users* here under Access Restriction on Users.

Step 8: **Scroll to Console Access Server Section.**
You can configure the following parameters here:

- all.sttyCmd
- all.poll_interval
- all.tx_interval
- all.idletimeout

Step 9: **Configure s<n>.serverfarm.**
This parameter will not appear on the configuration page when “All ports” is selected. Scroll to the SSH section. Each port can be named after the server or device connected to it. This makes the process of associating what is connecting to which port easier.

Step 10: **Click the Submit button.**
This will take you back to the Port Selection page. At this point, the configuration file is written in the RAMdisk.
Chapter 3 - Additional Features

Step 11: Click on the Serial Port Groups link on the Link Panel.
Click the Add Group button that appears. A Serial Ports - Users Group Table Entry page appears.

![Add Serial Ports - Users Group Table Entry](image)

*Figure 21: Serial Ports - Users Group Table Entry page*

Step 12: Configure conf.group.
Fill in the Group Name and Users fields to configure the group.

Step 13: Click the Submit button.
At this point, the configuration file is written in the RAMdisk.

Step 14: Make the changes effective.
Click on the Administration > Run Configuration link, check the Serial Ports/ Ethernet/Static Routes box and click on the Activate Configuration button.

Step 15: Save it in the flash.
Go to the link Administration > Load/Save Configuration and click the Save to Flash button.

Wizard Method

Step 1: Bring up the wizard.
At the command prompt, type the following to bring up the Access Method custom wizard:

```
wiz --ac cas
```
This will bring up Screen 1:

Screen 1:

***********************************************************
********* C O N F I G U R A T I O N W I Z A R D ***********
***********************************************************

INSTRUCTIONS for using the Wizard:
You can:
1) Enter the appropriate information for your system
and press ENTER. Enter '#' if you want to
deactivate that parameter 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...

Screen 2:

***********************************************************
********* C O N F I G U R A T I O N W I Z A R D ***********
***********************************************************

Current configuration:
(The ones with the '#' means it's not activated.)

all.ipno : #
all.socket_port : 7001+
all.protocol : socket_server
all.users : #
all.poll_interval : #
all.tx_interval : #
Chapter 3 - Additional Features

all.idletimeout : #
conf.group : #

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

Screen 3:

***********************************************************
********* C O N F I G U R A T I O N   W I Z A R D ***********
***********************************************************

ALL.IPNO - This is the default IP address of the system's
serial ports. If configured as 192.168.1.101+, the '+'
indicates that the first port should be addressed as
192.168.1.101 and the following ports should have
consecutive values. Any host can access a port using
its IP address as long as a path to the address exists
in the host's routing table.

all.ipno[#] :

ALL.SOCKET_PORT - This defines an alternative labeling
system for the system ports. The '+' after the numerical
value causes the interfaces (or ports) to be numbered
consecutively.
(e.g. interface 1 of your system is assigned port 7001,
interface 2 has the value 7002, etc.)

all.socket_port[7001+] :
**Screen 4:**

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

ALL.PROTOCOL - The possible protocols are telnet, ssh1/ssh2, raw data, or modbus.
(e.g. socket_server -telnet protocol, socket_ssh -ssh1/ssh2 protocol, raw_data -used to exchange data in transparent mode; similar to socket_server mode but without telnet negotiation breaks to serial ports modbus -an application layer messaging protocol for client/server communication widely used for industrial automation, etc.)

all.protocol[socket_server] :

ALL.MODBUS_SMODE - Communication mode through the serial ports. This parameter is valid only if the protocol configured is modbus. If it is and this parameter is not configured, ASCII mode will be assumed.
(e.g. ascii -normal TX/RX mode, rtu -Remote Transmission mode where some time constraints are observed between characters while transmitting a frame)

all.modbus_smode[#] :

ALL.USERS - Restricts access to ports by user name. Only the users listed can access the port, or using a '!', all but the users listed can access the port. A single comma and spaces/tabs may be used between names. A comma may NOT appear between the '' and the first user name. The users may be local, Radius or TacacsPlus. User groups (defined with the parameter conf.group) can be used in combination with user names in the parameter list. Notice that these are common users, not administrators.
(e.g. !joe, mark, grp1 -the users, Joe, Mark, and members of grp1, cannot access the port.)

all.users[#] :
```
Chapter 3 - Additional Features

Screen 5:

***********************************************************
********* C O N F I G U R A T I O N  W I Z A R D ***********
***********************************************************

ALL.POLL_INTERVAL - Valid for protocols socket_server and raw_data. When not set to 0, this parameter sets the wait for a TCP connection keep-alive timer. If no traffic passes through the system for this period of time, the system will send a line status message to the remote device to see if the connection is still up. If not configured, default is 1000ms. If set to 0, line status messages will not be sent to the socket client.

all.poll_interval[#] :

Screen 6:

***********************************************************
********* C O N F I G U R A T I O N  W I Z A R D ***********
***********************************************************

ALL.IDLETIMEOUT - This parameter specifies how long (in minutes) a connection can remain inactive before it is cut off. If set to 0 (the default), the connection will not time out.

all.idletimeout[#] :

CONF.GROUP - Used to combine users into a group. This simplifies the parameter, all.users. You can define more than one group. (e.g. groupName: user1, user2)

conf.group[#] :sales: john, jane

Would you like to create another group? (y/n) [n] :

Screen 7:

***********************************************************
********* C O N F I G U R A T I O N  W I Z A R D ***********
***********************************************************

Current configuration:
(The ones with the '#' means it's not activated.)

all.ipno : #
all.socket_port : 7001+
all.protocol : socket_server
all.modbus_smode : #
all.users : #
all.poll_interval : #
all.tx_interval : #
all.idletimeout : #
conf.group : #

Are these configuration(s) all correct? (y/n) [n]:

If you type 'n':
Type 'c' to go back and CORRECT these parameters or 'q' to QUIT :

Typing 'c' repeats the application, typing 'q' exits the entire wiz application.

If you type 'y':
Discard previous port-specific parameters? (y/n) [n] :
Chapter 3 - Additional Features

Type 'c' to CONTINUE to set these parameters for specific ports or 'q' to QUIT :

Typing 'c' leads to Screen 8, typing 'q' leads to Screen 9.

Screen 8:

***********************************************************
********* C O N F I G U R A T I O N   W I Z A R D ***********
***********************************************************

You have 8 available ports on this system.

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

Note: Answering yes to this question will discard only the parameter(s) which you are currently configuring if they were configured for a specific port in a previous session. For instance, if you are currently configuring parameter, all.x, and there was a specific port, s2.x, configured; then, answering yes to this question will discard s2.x.

Note: The number of available ports depends on the system you are on. Typing in a valid port number repeats this program except this time it's configuring for the port number you have chosen. For “wiz –ac cas,” an additional parameter is asked: serverfarm. Typing 'q' leads to Screen 9.
Screen 9:

***********************************************************
********* CONFIGURATION WIZARD *********
***********************************************************

(Note: If you are NOT connected to this unit through a console, and you have just reconfigured the IP of this unit, activating the new configurations may cause you to lose connection. In that case, please reconnect to the unit by the new IP address, and manually issue a saveconf to save your configurations to flash.)

Do you want to activate your configurations now? (y/n) [y] :

Screen 10:

***********************************************************
********* CONFIGURATION WIZARD *********
***********************************************************

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.

If you choose to save to flash, your configurations thus far will still be in the memory of the system even after you reboot it. If you don't save to flash and if you were to reboot the system, all your new configurations will be lost and you will have to reconfigure the system.

Do you want to save your configurations to flash? (y/n) [n] :

CLI Method

To configure certain parameters for a specific serial port:
Step 1: At the command prompt, type in the appropriate command to configure desired parameters.

To activate the serial port. <string> should be ttyS<serial port number>:

```
config configure line <serial port number> tty <string>
```

To configure the ipno:

```
config configure line <serial port number> ipno <string>
```

To configure the socket_port:

```
config configure line <serial port number> socket <number>
```

To configure the protocol. <string> is the type of protocol desired:

```
config configure line <serial port number> protocol <string>
```

To configure modbus_smode:

```
config configure line <serial port number> modbus <string>
```

To configure users:

```
config configure line <serial port number> users <string>
```

To configure the poll_interval:

```
config configure line <serial port number> pollinterval <number>
```

To configure tx_interval:

```
config configure line <serial port number> txinterval <number>
```

To configure idletimeout:

```
config configure line <serial port number> idletimeout <number>
```
To configure conf.group:

```
config configure conf group <string>
```

**Tip.** You can configure all the parameters for a serial port in one line.

```
config configure line <serial port number> tty <string>
ipno <string> socket <number> protocol <string>
modbus <string> users <string> pollinterval <number>
txinterval <number> idletimeout <number>
```

**Step 2: Activate and Save.**

To activate your new configurations and save them to flash, type:

```
config write
```
Chapter 3 - Additional Features

Configuration for TS

Parameters and Passed Values

For TS configuration, you will need to configure the following parameters:

- `all.host`: The IP address of the host to which the terminals will connect.

- `all.protocol`: For the terminal server configuration, the possible protocols are login (which requests username and password), rlogin (receives username from the TS and requests a password), telnet, ssh, ssh2, or socket_client. If the protocol is configured as telnet or socket_client, the parameter `socket_port` needs to be configured.

- `all.socket_port`: This parameter is valid only if `all.protocol` is configured as socket_client or telnet. The `socket_port` is the TCP port number of the application that will accept connections requested by this serial port.

- `all.telnet_client_mode`: When the protocol is TELNET, this parameter configured as BINARY (1) causes an attempt to negotiate the TELNET BINARY option on both input and output with the Telnet server. So it puts the telnet client in binary mode. The acceptable values are "0" or "1", where "0" is text mode (default) and "1" is a binary mode.

- `all.userauto`: Username used when connected to a UNIX server from the user's serial terminal. (unique to TS)

vi Method

The parameters described above must be changed by directly editing the `/etc/portslave/pslave.conf` file.
Access Method

Browser Method

Step 1: Follow the steps 1 to 4 in the section titled Configuration for CAS, "Browser Method" on page 88.

Step 2: Click the TS Profile button in the Wizard section.
   Configure the following parameters:

   \[ \text{Profile section:} \quad \begin{array}{c}
   \text{Protocol (telnet, ssh, rlogin or socket client)} \\
   \text{Socket port (23 for telnet, 22 for ssh, 513 for rlogin)}
   \end{array} \]

   \[ \text{Terminal Server section:} \quad \begin{array}{c}
   \text{Host (the name or the IP address of the host)} \\
   \text{Automatic User}
   \end{array} \]

Step 3: Click the Submit button.
   At this point, the configuration file is written in the RAMdisk.

Step 4: Make changes effective.
   Click on the Administration > Run Configuration link, check the Serial Ports/Ethernet/Static Routes box and click on the Activate Configuration button.

Step 5: Save it in the flash.
   Go to the link Administration > Load/Save Configuration and click the Save to Flash button.

Wizard Method

Step 1: Bring up the wizard.
   At the command prompt, type the following to bring up the Access Method custom wizard:

   \[ \text{wiz \ --ac \ ts} \]

   This will bring up Screen 1:
Chapter 3 - Additional Features

Screen 1:

***********************************************************
********* C O N F I G U R A T I O N W I Z A R D *********
***********************************************************

INSTRUCTIONS for using the Wizard:
You can:
1) Enter the appropriate information for your system
and press ENTER. Enter '#' if you want to
deactivate that parameter 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...

Screen 2:

***********************************************************
********* C O N F I G U R A T I O N W I Z A R D *********
***********************************************************

Current configuration:
(The ones with the '#' means it's not activated.)

all.protocol : rlogin
all.socket_port : 23
all.telnet_client_mode : 0
all.userauto : #

Set to defaults? (y/n) [n] : 
Screen 3:

***********************************************************
******* CONFIGURATION WIZARD *************
***********************************************************

ALL.PROTOCOL - Users can access the servers through the serial port using ssh, ssh2, telnet, login, rlogin, or socket_client.
(e.g. login -requests username and password, rlogin - receives username from the system and requests a password, etc.)

all.protocol[rlogin] :

ALL.SOCKE T_PORT - This defines the port(s) to be used by the protocols telnet and socket_client. For these two protocols a default value of 23 is used when no value is configured.

all.socket_port[23] :

Screen 4:

***********************************************************
******* CONFIGURATION WIZARD *************
***********************************************************

ALL.TELNET_CLIENT_MODE - This parameter only applies if the current protocol configured is telnet. Configuring as binary (1) causes an attempt to negotiate the TELNET BINARY option on both input and output with the Telnet server. Thus, it puts the telnet client in binary mode. The default is 0 which represents text mode.

all.telnet_client_mode[0] :
ALL.USERAUTO - Username used when connected to a Unix server from the user's serial terminal.

all.userauto[#] :

---

**Note:** all.host is configured under the wiz -- tso.

---

Screen 5:

********************************************************************************
********** CONFIGURATION WIZARD **********
********************************************************************************

Current configuration:
(The ones with the '#' means it's not activated.)

all.protocol : rlogin
all.socket_port : 23
all.telnet_client_mode : 0
all.userauto : #

Are these configuration(s) all correct? (y/n) [n]:

If you type 'n'
Type 'c' to go back and CORRECT these parameters or 'q' to QUIT :

Typing 'c' repeats the application, typing 'q' exits the entire wiz application

If you type 'y'
Discard previous port-specific parameters? (y/n) [n] :
Access Method

Note: Answering yes to this question will discard only the parameter(s) which you are currently configuring if they were configured for a specific port in a previous session. For instance, if you are currently configuring parameter, all.x, and there was a specific port, s2.x, configured; then, answering yes to this question will discard s2.x.

Type 'c' to CONTINUE to set these parameters for specific ports or 'q' to QUIT :

Typing 'c' leads to Screen 6, typing 'q' leads to Screen 7.

Screen 6:
******************************************************************************
********* C O N F I G U R A T I O N  W I Z A R D *********
******************************************************************************

You have 8 available ports on this system.

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

Note: The number of available ports depends on the system you are on. Typing in a valid port number repeats this program except this time it's configuring for the port number you have chosen. Typing 'q' leads to Screen 7.
Chapter 3 - Additional Features

Screen 7:

***********************************************************
********* C O N F I G U R A T I O N  W I Z A R D ***********
***********************************************************

(Note: If you are NOT connected to this unit through a console, and you have just reconfigured the IP of this unit, activating the new configurations may cause you to lose connection. In that case, please reconnect to the unit by the new IP address, and manually issue a saveconf to save your configurations to flash.)

Do you want to activate your configurations now? (y/n) [y] :

Screen 8:

***********************************************************
********* C O N F I G U R A T I O N  W I Z A R D ***********
***********************************************************

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.

If you choose to save to flash, your configurations thus far will still be in the memory of the system even after you reboot it. If you don't save to flash and if you were to reboot the system, all your new configurations will be lost and you will have to reconfigure the system.

Do you want to save your configurations to flash? (y/n) [n] :
CLI Method
To configure certain parameters for a specific serial port:

**Step 1:** At the command prompt, type in the appropriate command to configure desired parameters.

To activate the serial port. `<string>` should be ttyS<serial port number>:

```
config configure line <serial port number> tty <string>
```

To configure the protocol (`<string>` is the type of protocol desired):

```
config configure line <serial port number> protocol <string>
```

To configure the socket_port:

```
config configure line <serial port number> socket <number>
```

To configure the telnet_client_mode:

```
config configure line <serial port number> telnetclientmode <number>
```

To configure userauto:

```
config configure line <serial port number> userauto <string>
```

**Tip.** You can configure all the parameters for a serial port in one line.

```
config configure line <serial port number> tty <string> protocol <string> socket <number> telnetclientmode <number> userauto <string>
```

**Step 2:** Activate and Save.

To activate your new configurations and save them to flash, type:

```
config write
```

(This is essentially typing `signal_ras hup` and `saveconf` from the normal terminal prompt.)
Chapter 3 - Additional Features

Configuration for Dial-in Access

Parameters and Passed Values

The parameters that need to be configured are shown in the following list. *Note: The character “\” at the end of a line means that the string continues on the next line.*

- **conf.pppd**
  Location of the ppp daemon with Radius. Default value: `/usr/local/sbin/pppd`.

- **all.ipno**
  This is the default IP address of the 's serial ports. Any host can access a port using its IP address as long as a path to the address exists in the host's routing table. An example value would be 192.168.1.101+. The “+” indicates that the first port should be addressed as 192.168.1.101 and the following ports should have consecutive values.

- **all.initchat**
  Modem initialization string. Example value:

  ```
  TIMEOUT 10 "\d\n\dATZ\OK\r\n-ATZ-OK\r\n" "%" ATMO OK\r\n "%" \n
  TIMEOUT 3600 RING "" \n
  STATUS Incoming %p:I.HANDSHAKE "" ATA\n
  TIMEOUT 60 CONNECT@ "" \n
  STATUS Connected %p:I.HANDSHAKE
  ```

- **all.autopp**
  Options to auto-detect a ppp session. The cb-script parameter defines the file used for callback and enables negotiation with the callback server. Callback is available in combination with Radius Server authentication.

  When a registered user calls the Cyclades-TS, it will disconnect the user, then call the user back. The following three parameters must be configured in the Radius Server:

  - **attribute Service_type(6): Callback Framed**;
  - **attribute Framed_Protocol(7): PPP**;
  - **attribute Callback_Number(19): the dial number (example: 50903300)**.
Create an user PAP or CHAP

You also have to create a user in `/etc/ppp/pap-secrets` or in `/etc/ppp/chap-secrets`, depending if you want PAP or CHAP authentication. You will also have to create a user in `/etc/ppp/pap-secrets` or in `/etc/ppp/chap-secrets`.
secrets if you want radius or local authentication. In case you don't want to repeat all the user
database from the radius server an option is to use ‘*’ as the user in /etc/ppp/pap-secrets:

```
*     *     ""     *
```

**Tip.** Documentation about PPP options can be found on the Linux pppd man
page.

*vi Method*

The parameters described above must be changed by directly editing the /etc/portslave/
pslave.conf file.

*Browser Method*

For the serial ports you would have all the parameters described above but conf.*.
To configure Access Method with your browser:

**Step 1:** Follow the steps 1 to 4 in the section titled Configuration for CAS, “Browser
Method” on page 88.

**Step 2:** Click the Dial in Profile button in the Wizard section.

**Step 3:** Scroll down to the Profile section.
You can change the settings for all.ipno and all.protocol in this section.

**Step 4:** Scroll to the modem Section.
You can configure the parameter all.initchat here.

**Step 5:** Scroll to the PPP Section.
You can configure the parameter all.autopp and all.pppopt here.

**Step 6:** Click the Submit button.
At this point, the configuration file is written in the RAMdisk.

**Step 7:** Make the changes effective.
Click on the Administration > Run Configuration link, check the Serial Ports/Ethernet/Static Routes box and click on the Activate Configuration button.

**Step 8: Save it in the flash.**

Go to the link Administration > Load/Save Configuration and click the Save to Flash button.
Chapter 3 - Additional Features

CLI Method
To configure certain parameters for a specific serial port:

**Step 1:** At the command prompt, type in the appropriate command to configure desired parameters.

To activate the serial port. <string> should be ttyS<serial port number>:

```bash
config configure line <serial port number> tty <string>
```

To configure the protocol. <string> is the type of protocol desired:

```bash
config configure line <serial port number> protocol <string>
```

To configure ipno:

```bash
config configure line <serial port number> ipno <string>
```

**Tip.** You can configure all the parameters for a serial port in one line.

```bash
config configure line <serial port number> tty <string> protocol <string> ipno <string>
```

**Step 2:** Activate and Save.
To activate your new configurations and save them to flash, type:

```bash
config write
```

(This is essentially typing `signal_ras bup` and `saveconf` from the normal terminal prompt.)
Authentication

Authentication is the process of identifying an individual, usually based on a username and password. In security systems, authentication is distinct from authorization, which is the process of giving individuals access to system objects based on their identity. Authentication merely ensures that the individual is who he or she claims to be, but says nothing about the access rights of the individual. With the Cyclades-TS, authentication can be performed locally, or with a remote Radius, Tacacs, or ldap database.

Parameters Involved and Passed Values

The authentication feature utilizes the following parameters:

\[ all.authtype \]

<table>
<thead>
<tr>
<th>Type of authentication used. There are several authentication type options:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• \textit{none} (no authentication)</td>
</tr>
<tr>
<td>• \textit{local} (authentication is performed using the \texttt{/etc/passwd} file)</td>
</tr>
<tr>
<td>• \textit{remote} (This is for a terminal profile only. The unit takes in a username but does not use it for authentication. Instead it passes it to the remote server where it is then used for authentication.)</td>
</tr>
<tr>
<td>• \textit{radius} (authentication is performed using a Radius authentication server)</td>
</tr>
<tr>
<td>• \textit{TacacsPlus} (authentication is performed using a TacacsPlus authentication server)</td>
</tr>
<tr>
<td>• \textit{ldap} (authentication is performed against an ldap database using an ldap server. The IP address and other details of the ldap server are defined in the file \texttt{/etc/ldap.conf})</td>
</tr>
</tbody>
</table>
Chapter 3 - Additional Features

- **local/radius** (authentication is performed locally first, switching to Radius if unsuccessful)
- **radius/local** (the opposite of the previous option)
- **local/TacacsPlus** (authentication is performed locally first, switching to TacacsPlus if unsuccessful)
- **TacacsPlus/local** (the opposite of the previous option)
- **RadiusDownLocal** (local authentication is tried only when the Radius server is down)
- **TacacsPlusDownLocal** (local authentication is tried only when the TacacsPlus server is down)
- **ldapDownLocal** (local authentication is tried only when the ldap server is down)
- **NIS** - All authentication types but NIS follow the format all.authtype <Authentication>DownLocal or <Authentication> (e.g. all.authtype radius or radiusDownLocal or ldap or ldapDownLocal, etc). NIS requires all.authtype to be set as local, regardless if it will be "nis" or its "Downlocal" equivalent. The service related to "nis" or its "Downlocal" equivalent would be configured in the /etc/nsswitch.conf file, not in the /etc/portslave/pslave.conf file.

Note that this parameter controls the authentication required by the Cyclades-TS. The authentication required by the device to which the user is connecting is controlled separately.

**all.authhost1**

**all.authhost2**

This address indicates the location of the Radius/TacacsPlus authentication server and is only necessary if this option is chosen in the previous parameter. A second Radius/TacacsPlus authentication server can be configured with the parameter all.authhost2.
Authentication

**all.accthost1**  This address indicates the location of the Radius/TacacsPlus accounting server, which can be used to track how long users are connected after being authorized by the authentication server. Its use is optional. If this parameter is not used, accounting will not be performed. If the same server is used for authentication and accounting, both parameters must be filled with the same address. A second Radius/TacacsPlus accounting server can be configured with the parameter all.accthost2.

**all.accthost2**

**all.radtimeout**  This is the timeout (in seconds) for a Radius authentication query to be answered.

**all.radretries**  Defines the number of times each Radius/TacacsPlus server is tried before another is contacted. The first server (authhost1) is tried “radretries” times, and then the second (authhost2), if configured, is contacted “radretries” times. If the second also fails to respond, Radius/TacacsPlus authentication fails.

**all.secret**  This is the shared secret (password) necessary for communication between the Cyclades-TS and the Radius/TacacsPlus servers.

Configuration for CAS, TS, and Dial-in Access

**vi Method**

The parameters described above must be changed by directly editing the /etc/portslave/pslave.conf file.

**Browser Method**

To configure Authentication with your browser:

**Step 1:** Follow the steps 1 to 4 in the section titled Configuration for CAS, “Browser Method” on page 88.

**Step 2:** Scroll to the Authentication section.

Scroll down to the Authentication section and configure the parameters in this section.

**Step 3:** Click the Submit button.

At this point, the configuration file is written in the RAMdisk.
Chapter 3 - Additional Features

Step 4: Make changes effective.
Click on the Administration > Run Configuration link, check the Serial Ports/Ethernet/Static Routes box and click on the Activate Configuration button.

Step 5: Save it in the flash.
Go to the link Administration > Load/Save Configuration and click the Save to Flash button.

Wizard Method

Step 1: Bring up the wizard.
At the command prompt, type the following to bring up the Authentication custom wizard:

```
wiz --auth
```

Screen 1 will appear.

Screen 1:

```
***********************************************************
********* C O N F I G U R A T I O N   W I Z A R D ***********
***********************************************************
```

INSTRUCTIONS for using the Wizard:
You can:
1) Enter the appropriate information for your system and press ENTER. Enter '#' if you want to deactivate that parameter 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...
Screen 2:

*****************************************************************************
********** CONFIGURATION WIZARD **********
*****************************************************************************

Current configuration:
(The ones with the '#' means it's not activated.)

all.authtype : none
all.authhost1 : 192.168.160.3
all.accthost1 : 192.168.160.3
all.authhost2 : 192.168.160.4
all.accthost2 : 192.168.160.4
all.radtimeout : 3
all.radretries : 5
all.secret : secret

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

Screen 3:

*****************************************************************************
********** CONFIGURATION WIZARD **********
*****************************************************************************

ALL.AUTHTYPE - This parameter controls the authentication required by the system. Users' access to the server through the serial port is granted through the check of username and password locally or remotely. (e.g. none, local, TacacsPlus (note the capital 'T' in TacacsPlus), radius, ldap, etc.

all.authtype[none] : 
ALL.AUTHHOST1 - This IP address indicates where the Radius or TacacsPlus authentication server is located.

all.authhost1[200.200.200.2] :

Screen 4:

***********************************************************
********* C O N F I G U R A T I O N W I Z A R D ***********
***********************************************************

ALL.ACCTHOST1 - This IP address indicates where the Radius or TacacsPlus accounting server is located. The accounting server can be used to track how long users are connected after being authorized by the authentication server.

all.accthost1[200.200.200.3] :

ALL.AUTHHOST2 - This IP address indicates where the SECOND Radius or TacacsPlus authentication server is located.

all.authhost2[200.200.200.2] :

Note: If authtype is configured as none, local, or ldap, the application will skip immediately to the summary screen because the rest of the parameters pertain only if the system is configured to use a Radius or TacacsPlus server. Configurations for ldap are done in /etc/ldap.conf.
Screen 5:
***********************************************************
********* C O N F I G U R A T I O N  W I Z A R D *********
***********************************************************

ALL.ACCTHOST2 - This IP address indicates where the SECOND Radius or TacacsPlus accounting server is located.

all.accthost2[200.200.200.3] :

ALL.RADTIMEOUT- This is the timeout (in seconds) for a Radius or TacacsPlus authentication query to be answered.

all.radtimeout[3] :

Screen 6:
***********************************************************
********* C O N F I G U R A T I O N  W I Z A R D *********
***********************************************************

ALL.RADRETRIES - This defines the number of times each Radius or TacacsPlus server is tried before another is contacted.

all.radretries[5] :

ALL.SECRET - This is the shared secret necessary for communication between the system and the Radius or TacacsPlus servers.

all.secret[secret] :
Screen 7:
***********************************************************
********* C O N F I G U R A T I O N  W I Z A R D ***********
***********************************************************
Current configuration:
(The ones with the '#' means it's not activated.)

all.authtype : none
all.authhost1 : 200.200.200.2
all.accthost1 : 200.200.200.3
all.authhost2 : 200.200.200.2
all.accthost2 : 200.200.200.3
all.radtimeout : 3
all.radretries : 5
all.secret : rad-secret

Are these configuration(s) all correct? (y/n) [n] :

If you type 'n'
Type 'c' to go back and CORRECT these parameters or 'q' to QUIT :

Typing 'c' repeats application, typing 'q' exits the entire wiz application

If you type 'y'
Discard previous port-specific parameters? (y/n) [n] :

Note: Answering yes to this question will discard only the parameter(s) which you are currently configuring if they were configured for a specific port in a previous session. For instance, if you are currently configuring parameter, all.x, and there was a specific port, s2.x, configured; then, answering yes to this question will discard s2.x.

Type 'c' to CONTINUE to set these parameters for specific ports or 'q' to QUIT :
Typing 'c' leads to Screen 8, typing 'q' leads to Screen 9.

Screen 8:

***********************************************************
********* C O N F I G U R A T I O N W I Z A R D ***********
***********************************************************
You have 8 available ports on this system.

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

**Note:** The number of available ports depends on the system you are on. Typing in a valid port number repeats this program except this time it's configuring for the port number you have chosen. Typing 'q' leads to Screen 9.

Screen 9:

***********************************************************
********* C O N F I G U R A T I O N W I Z A R D ***********
***********************************************************

(Note: If you are NOT connected to this unit through a console, and you have just reconfigured the IP of this unit, activating the new configurations may cause you to lose connection. In that case, please reconnect to the unit by the new IP address, and manually issue a saveconf to save your configurations to flash.)

Do you want to activate your configurations now? (y/n) [y] :
Screen 10:
***********************************************************
********* CONFIGURATION WIZARD *********
***********************************************************

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.

If you choose to save to flash, your configurations thus far will still be in the memory of the system even after you reboot it. If you don't save to flash and if you were to reboot the system, all your new configurations will be lost and you will have to reconfigure the system.

Do you want to save your configurations to flash? (y/n) [n] :
Authentication

CLI Method
To configure certain parameters for a specific serial port.

**Step 1**: At the command prompt, type in the appropriate command to configure desired parameters.

To activate the serial port. `<string>` should be `ttyS<serial port number>`:

```
config configure line <serial port number> tty <string>
```

To configure authtype:

```
config configure line <serial port number> authtype <string>
```

To configure authhost1:

```
config configure line <serial port number> authhost1 <string>
```

To configure accthost1:

```
config configure line <serial port number> accthost1 <string>
```

To configure authhost2:

```
config configure line <serial port number> authhost2 <string>
```

To configure accthost2:

```
config configure line <serial port number> accthost2 <string>
```

To configure radtimeout:

```
config configure line <serial port number> timeout <number>
```

To configure radretries:

```
config configure line <serial port number> retries <number>
```
Chapter 3 - Additional Features

To configure secret:

```bash
config configure line <serial port number> secret <string>
```

**Tip.** You can configure all the parameters for a serial port in one line.

```bash
config configure line <serial port number> tty <string> authtype <string> authhost1 <string> accthost1 <string> authhost2 <string> accthost2 <string> timeout <number> retries <number> secret <string>
```

**Step 2: Activate and Save.**

To activate your new configurations and save them to flash, type:

```bash
config write
```

**Access Control via Radius Attribute NAS-Port-id**

This feature provides an additional way to control the access to serial ports other than the one based in usernames or groups. The authentication type must be Radius for this feature to function. The Radius server administrator must configure the user (in the radius server database) with one NAS-PORT-Id attribute for each serial port that the user is allowed to access.

In the example below the user alfred can access the serial ports ttyS11, ttyS13, and ttyS17:

```
alfred Auth-Type = Local, Password = 'alfred'

Service-Type = Framed-User,
Framed-Protocol = PPP,
NAS-Port-Id = 11,
NAS-Port-Id = 13,
NAS-Port-Id = 17
```
The pam_radius module will check whether the NAS-Port-Id matches one of those sent by the radius server. If the radius server does not send the NAS-Port-Id attribute, no check is performed.

No configuration is needed for the AlterPath Console Server or the Cyclades-TS. However, the authentication type must be “radius”. Authentications like radiusDownLocal, radius/local, etc. will not validate the NAS-port-Id if the user was locally authenticated.

This feature is available for the , TS 1.3.7 onward. CAS Port Pooling allows you to access a free serial port from a pool in addition to the original feature where you could access a specific serial port. When you access a serial port through the pool the features sniff session and multiple sessions are not available. This feature is available for serial ports configured as CAS profile only.

You can define more than one pool of serial ports. Each serial port can only belong to ONE pool. The pool is uniquely identified by a four parameter scheme:

- protocol,
- pool_ipno,
- pool_serverfarm, and
- pool_socket_port

The three new parameters: pool_ipno, pool_serverfarm, and pool_socket_port have the same meaning as ipno, serverfarm, and socket_port respectively. Ports belonging to the same pool MUST be configured with the same value in these fields.

It is strongly recommended that you configure the same values in all parameters related to authentication for all serial ports belonging to a pool. Some of the authentication parameters are users, admin_users, and authtype.

You can access the serial ports from a pool with the same commands you use today to access a specific serial port. You just need to use pool_ipno, pool_serverfarm, or pool_socket_port instead ipno, serverfarm, or socket_port respectively in the ssh/telnet command.
When a connection request arrives using one of pool_ipno, pool_serverfarm, or pool_socket_port the TS will look for the first free serial port from the pool and that port will be assigned to connection. If there is no serial port free in the pool the connection is just dropped.

**How to Configure it**

Following is an example of serial port pool configuration:

```
#  
# Serial port pool: pool-1
#

s1.tty ttyS1
s1.protocol socket_server
s1.socket_port 7001 // TCP port # for specific allocation
s1.pool_socket_port 3000 // TCP port # for the pool
s1.ipno 10.0.0.1 // IP address for specific allocation
s1.pool_ipno 10.1.0.1 // IP address for the pool
s1.serverfarm serial-1 // alias for specific allocation
s1.pool_serverfarm pool-1 // alias for the pool

s2.tty ttyS2
s2.protocol socket_server
s2.socket_port 7002 // TCP port # for specific allocation
s2.pool_socket_port 3000 // TCP port # for the pool
s2.ipno 10.0.0.2 // IP address for specific allocation
s2.pool_ipno 10.1.0.1 // IP address for the pool
s2.serverfarm serial-2 // alias for specific allocation
s2.pool_serverfarm pool-1 // alias for the pool

#  
# Serial port pool: pool-2
#

s3.tty ttyS3
s3.protocol socket_ssh
s3.socket_port 7003 // TCP port # for specific allocation
s3.pool_socket_port 4000 // TCP port # for the pool
s3.ipno 10.0.0.3 // IP address for specific allocation
s3.pool_ipno 10.2.0.1 // IP address for the pool
```
s3.serverfarm serial-3 // alias for specific allocation
s3.pool_serverfarm pool-2 // alias for the pool

s4.tty ttyS4
s4.protocol socket_ssh
s4.socket_port 7004 // TCP port # for specific allocation
s4.pool_socket_port 4000 // TCP port # for the pool
s4.ipno 10.0.0.4 // IP address for specific allocation
s4.pool_ipno 10.2.0.1 // IP address for the pool
s4.serverfarm serial-4 // alias for specific allocation
s4.pool_serverfarm pool-2 // alias for the pool

In the example above, there are two pools:

- **pool-1** (identified by Protocol socket_server, TCP port #3000, IP 10.1.0.1, and alias pool-1)
- **pool-2** (identified by Protocol socket_ssh, TCP port #4000, IP 10.2.0.1, and alias pool-2)

The serial ports ttyS1 and ttyS2 belong to the pool-1. The serial ports ttyS3 and ttyS4 belong to the pool-2.

You can access specifically serial port ttyS1 by using TCP port 7001, IP address 10.0.0.1 or alias serial-1. If the ttyS1 is being used by somebody else the connection will be dropped if the user is not a admin_user. Alternately, you can access ttyS1 through pool (if it's free) using TCP port 3000, IP 10.1.0.1 or alias pool-1. If it is not free ttyS2 will be automatically allocated. Additionally, if ttyS2 is not free, the connection will be dropped.
Chapter 3 - Additional Features

Centralized Management

The Cyclades-TS allows centralized management through the use of a Master pslave.conf file. Administrators should consider this approach to configure multiple Cyclades-TS. Using this feature, each unit has a simplified pslave.conf file where a Master include file is cited. This common configuration file contains information for all units, properly divided in separate sections, and would be stored on one central server. This file, in our example shown in the following figure Figure 22: Example of Centralized Management, is /etc/portslave/TScommon.conf. It must be downloaded to each Cyclades-TS.

Note: Centralized management can mean one big configuration file (the common file) that is placed in a management host. This same file would be downloaded into all TS boxes (each of those boxes would include a tiny config file and that big common file). In this application, there may or may not be clustering involved. The user may want to access each box individually, without passing through a central point (master), using the common file just to make his/her life easier in regard to maintain the config file. This user could ALSO add the clustering application on a daily basis. Clustering does NOT require a common config file. A common config file does NOT apply to clustering, however, common config files can be used in an integrated manner.

Figure 22: Example of Centralized Management

The abbreviated pslave.conf and /etc/hostname files in each unit, for the example are:

- Cyclades-TS Unit 1
  IP address: 10.0.0.1/8
- Cyclades-TS Unit 2
  IP address: 10.0.0.2/8
- Cyclades-TS Unit 3
  IP address: 10.0.0.3/8

Server where master configuration file is stored
/etc/portslave/TScommon.conf
For the /etc/hostname file in **unit 1**:

unit1

For the plsave.conf file in **unit 1**:

conf.eth_ip 10.0.0.1
conf.eth_mask 255.0.0.0
conf.include /etc/portslave/TScommon.conf

For the /etc/hostname file in **unit 2**:

unit2

For the plsave.conf file in **unit 2**:

conf.eth_ip 10.0.0.2
conf.eth_mask 255.0.0.0
conf.include /etc/portslave/TScommon.conf

For the /etc/hostname file in **unit 3**:

unit3

For the plsave.conf file in **unit 3**:

conf.eth_ip 10.0.0.3
conf.eth_mask 255.0.0.0
conf.include /etc/portslave/TScommon.conf

The common include file for the example is:

all.authtype none
all.protocol socket_server
conf.host_config unit1
all.socket_port 7001+
s1.tty  ttyS1
s2.tty  ttyS2
...
s16.tty  ttyS16
s17.tty  20.20.20.3:7033
s18.tty  20.20.20.3:7034
...
conf.host_config unit2
all.socket_port 7033+
s1.tty  ttyS1
s2.tty  ttyS2
...
sN.tty  ttySN
conf.host_config unit3
all.socket_port 7301+
s1.tty  ttyS1
s2.tty  ttyS2
...
sN.tty  ttySN
conf.host_config end
Centralized Management

When this file is included, unit1 would read only the information between
\texttt{conf.host\_config unit1} and \texttt{conf.host\_config unit2}. Unit2 would use only the information
between \texttt{conf.host\_config unit2} and \texttt{conf.host\_config unit3} and unit3 would use information
after \texttt{conf.host\_config unit3} and before \texttt{conf.host\_config end}.

Steps for using Centralized Configuration

**Step 1:** Create and save the \texttt{/etc/portslave/pslave.conf} and \texttt{/etc/hostname} files in each
Cyclades-TS.

**Step 2:** Create, save, and download the common configuration.
Create and save the common configuration file on the server, then download it
(probably using \texttt{scp}) to each unit. Make sure to put it in the directory set in the
\texttt{pslave.conf} file (\texttt{/etc/portslave} in the example).

**Step 3:** Execute the command \texttt{signal\_ras hup} on each unit.

**Step 4:** Test each unit.
If everything works, add the line \texttt{/etc/portslave/TScommon.conf} to the
\texttt{/etc/config\_files} file.

**Step 5:** Save the file and close it.

**Step 6:** Execute the \texttt{saveconf} command.

\begin{center}
\begin{tabular}{|c|}
\hline
\textbf{Note:} The included file \texttt{/etc/portslave/TScommon.conf} cannot contain another
include file (i.e., the parameter \texttt{conf.include} must not be defined).
\hline
\end{tabular}
\end{center}

Also, \texttt{<max ports of TS> + N(+) is done same way as serial port.}
Chapter 3 - Additional Features

Clustering

Clustering is available for the Cyclades-TS with firmware versions 1.3.0 and up (except for the TS110/100). It allows the stringing of Terminal Servers so that one Master Cyclades-TS can be used to access all Cyclades-TSs on a LAN. The Master Cyclades-TS can manage up to 1024 serial ports, so that the following can be clustered:

- 1 Master TS1000 + 31 Slave TS1000s, or
- 1 Master TS2000 + 15 Slave TS2000s, or
- 1 Master TS3000 + 9 slave TS3000s + 1 slave TS2000

An example with one Master TS2000 and two Slave TS1000s is shown in the following figure.

Figure 23: An example using the Clustering feature
Parameters Involved and Passed Values

The Master Cyclades-TS must contain references to the Slave ports. The configuration described earlier for Console Access Servers should be followed with the following exceptions for the Master and Slaves:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Value for this example</th>
</tr>
</thead>
<tbody>
<tr>
<td>conf.eth_ip</td>
<td>Ethernet Interface IP address.</td>
<td>20.20.20.1</td>
</tr>
<tr>
<td>conf.eth_ip_alias</td>
<td>Secondary IP address for the Ethernet Interface (needed for clustering feature).</td>
<td>209.81.55.110</td>
</tr>
<tr>
<td>conf.eth_mask_alias</td>
<td>Mask for secondary IP address above.</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>all.socket_port</td>
<td>This value applies to both the local ports and ports on Slave Cyclades-TS.</td>
<td>7001+</td>
</tr>
<tr>
<td>all.protocol</td>
<td>Depends on the application.</td>
<td>Socket_ssh or socket_server</td>
</tr>
<tr>
<td>all.authtype</td>
<td>Depends on the application.</td>
<td>Radius, local, none, remote, TacacsPlus, Ldap, local/Radius, radius/local, local/TacacsPlus, TacacsPlus, local, RadiusDownLocal, ldapDownLocal, NIS</td>
</tr>
<tr>
<td>s33.tty</td>
<td>This parameter must be created in the Master TS file for every Slave port. Its format is: IP_of_Slave:[slave_socket_port] for non-Master ports. In this case, the slave_socket_port value is not necessary because s33.socket_port is automatically set to 7033 by all.socket_port above.</td>
<td>20.20.20.2:7033</td>
</tr>
</tbody>
</table>
## Chapter 3 - Additional Features

### Table 7: Master Cyclades Configuration (where it differs from the CAS standard)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Value for this example</th>
</tr>
</thead>
<tbody>
<tr>
<td>s33.serverfarm</td>
<td>An alias for this port. (This is an optional parameter)</td>
<td>Server_on_slave1_serial_s1</td>
</tr>
<tr>
<td>s33.ipno</td>
<td>This parameter must be created in the Master TS file for every Slave port, unless configured using all.ipno.</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>s34.tty</td>
<td>See s33.tty.</td>
<td>20.20.20.2:7034</td>
</tr>
<tr>
<td>s34.serverfarm</td>
<td>An alias for this port.</td>
<td>Server_on_slave1_serial_s2</td>
</tr>
<tr>
<td>s34.ipno</td>
<td>See s33.ipno.</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>s35.tty</td>
<td>See s33.tty.</td>
<td>20.20.20.2:7035</td>
</tr>
<tr>
<td>s35.serverfarm</td>
<td>An alias for this port.</td>
<td>Server_on_slave1_serial_s3</td>
</tr>
<tr>
<td>s35.ipno</td>
<td>See s33.ipno.</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>etc. for s36-s64</td>
<td></td>
<td></td>
</tr>
<tr>
<td>s65.tty</td>
<td>The format of this parameter is IP_of_Slave:[slave_socket_port] for non-Master ports. The value 7301 was chosen arbitrarily for this example.</td>
<td>20.20.20.3:7301</td>
</tr>
<tr>
<td>s65.serverfarm</td>
<td>An alias for this port.</td>
<td>Server_on_slave2_serial_s1</td>
</tr>
<tr>
<td>s65.ipno</td>
<td>See s33.ipno.</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>s66.tty</td>
<td>See s65.tty</td>
<td>20.20.20.3:7302</td>
</tr>
<tr>
<td>s66.serverfarm</td>
<td>An alias for this port.</td>
<td>Server_on_slave2_serial_s2</td>
</tr>
<tr>
<td>s66.ipno</td>
<td>See s33.ipno.</td>
<td>0.0.0.0</td>
</tr>
</tbody>
</table>
The Slave Cyclades-TSs do not need to know they are being accessed through the Master Cyclades-TS. (You are creating virtual terminals: virtual serial ports.) Their port numbers, however, must agree with those assigned by the Master.

**Table 7: Master Cyclades Configuration (where it differs from the CAS standard)**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Value for this example</th>
</tr>
</thead>
<tbody>
<tr>
<td>S67.tty</td>
<td>See s65.tty.</td>
<td>20.20.20.3:7303</td>
</tr>
<tr>
<td>S67.serverfarm</td>
<td>An alias for this port.</td>
<td>Server_on_slave2_serial_s3</td>
</tr>
<tr>
<td>S67.ipno</td>
<td>See s33.ipno.</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>etc. for s68-s96</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Table 8: Cyclades-TS configuration for Slave 1 (where it differs from the CAS standard)**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value for this example</th>
</tr>
</thead>
<tbody>
<tr>
<td>all.protocol</td>
<td>socket_server</td>
</tr>
<tr>
<td>all.authtype</td>
<td>none</td>
</tr>
<tr>
<td>conf.eth_ip</td>
<td>20.20.20.2</td>
</tr>
<tr>
<td>all.socket_port</td>
<td>7033+</td>
</tr>
</tbody>
</table>
To access ports from the remote management workstation, use telnet with the secondary IP address:

telnet 209.81.55.110 7001
to access the first port of the Master Cyclades-TS.

telnet 209.81.55.110 7033
to access the first port of Slave 1.

telnet 209.81.55.110 7301
to access the first port of Slave 2.

Ssh can also be used from the remote management workstation:

ssh -l <username>:Server_on_slave2_serial_s3 209.81.55.110
to access the third port of Slave 2, or

ssh -l <username>:7305 209.81.55.110

to access the fifth port of Slave 2.

(Thus the Cyclades-TS family does not have this feature.)
CronD

CronD is a service provided by the Cyclades-TS system that allows automatic, periodically-run custom-made scripts. It replaces the need for the same commands to be run manually.

**Parameters Involved and Passed Values**

The following parameters are created in the `/etc/crontab_files` file:

- **status**: Active or inactive. If this item is not active, the script will not be executed.
- **user**: The process will be run with the privileges of this user, who must be a valid local user.
- **source**: Pathname of the crontab file that specifies frequency of execution, the name of shell script, etc. It should be set using the traditional crontab file format.

Example:
The name of the shell script with the commands to be executed is `/etc/teste_cron.sh`. The name of the crontab file is `/etc/crontab_tst` and it contains one line:

```
0-59 * * * * /etc/teste_cron.sh
```

Insert the follow line in the `/etc/crontab_files`:

```
active root /etc/crontab_tst
```

Result: CronD will execute the shell script teste_cron.sh with root privileges each minute.

**Note**: In `/etc/crontab`, you can only have one active entry per user. For instance, from the example above, you cannot add another active entry for root because it already has an entry. If you want to add more scripts, you can just add them to the source file (`/etc/crontab_tst`).
Chapter 3 - Additional Features

Configuration for CAS, TS, and Dial-in Access

**Important!** After creating the shell script and **crontab** file and modifying the **crontab_files** file, make sure the file named **/etc/config_files** contains the names of all files that should be saved to flash. Run the command **saveconf** after this confirmation.

vi Method
The files Crontab and shell script are created and the file **/etc/crontab_files** is modified as indicated.

To use cronD:

**Step 1:** Create the files for every process that it will execute:

**Step 2:** Create a line in the file **/etc/crontab_files** for each process to be run.

**Step 3:** Update the system.
The next step is to update the system with the modified data. Make sure the file named **/etc/config_files** contains the names of all files that should be saved to flash.

**Step 4:** Run **saveconf**.
The command **saveconf**, which reads the **/etc/config_files** file, should then be run. **saveconf** copies all the files listed in the file **/etc/config_files** from the ramdisk to **/proc/flash/script**.

**Step 5:** Reboot the Cyclades-TS.

Browser Method
To configure CronD with your browser:

**Step 1:** Point your browser to the Console Server.
In the address or location field of your browser type the Console Access Server's IP address. For example:

http://10.0.0.0
Step 2: Log in as root and type the Web root password configured by the Web server.
This will take you to the Configuration and Administration page.

Step 3: Click on the Edit Text File link.
Click on this link on the Link Panel. You can then pull up the appropriate file and edit it.

Figure 24: Edit Text File page

Data Buffering

Introduction
Data buffering can be done in local files or in remote files through NFS. When using remote files, the limitation is imposed by the remote Server (disk/partition space) and the data is kept in linear (sequential) files in the remote Server. When using local files, the limitation is imposed by the size of the available ramdisk. You may wish to have data buffering done in file, syslog or both. For syslog, `all.syslog_buffering` and `conf.DB_facility` are the parameters to be dealt with, and syslog-ng.conf file should be set accordingly. (Please see Syslog for the syslog-ng configuration file.) For the file, `all.data_buffering` is the parameter to be dealt with.

Conf.nfs_data_buffering is a remote network file system where databuffering will be written, instead of using the default directory /var/run/DB. When commented, it indicates local data buffering. The directory tree to which the file will be written must be NFS-mounted and the local path name is /mnt/DB_nfs. The remote host must have NFS installed and the administrator must create, export, and allow reading/writing to this directory. The size of this file is not limited by the value of the parameter s1.data_buffering, though the value cannot be zero since a zero value turns off data buffering.
Chapter 3 - Additional Features

The `conf.nfs_data_buffering` parameter format is:

```
<server name or IP address>:<remote pathname>
```

If data buffering is turned on for port 1, for example, the data will be stored in the file `ttyS1.data` (or `&lt;serverfarm1&gt;.data` if `s1.serverfarm` was configured) in local directory `/var/run/DB` or in remote path name and server indicated by the `conf.nfs_data_buffering`.

**Ramdisks**

Data buffering files are created in the directory `/var/run/DB`. If the parameter `s<nn>.serverfarm` is configured for the port `<nn>`, this name will be used. For example, if the serverfarm is called bunny, the data buffering file will be named `bunny.data`.

The shell script `/bin/build_DB_ramdisk` creates a 48 Mbyte ramdisk for the TS3000. Use this script as a model to create customized ramdisks for your environment. Any user-created scripts should be listed in the file `/etc/user_scripts` because `rc.sysinit` executes all shell scripts found there. This avoids changing `rc.sysinit` itself.

**Linear vs. Circular Buffering**

For local data buffering, this parameter allow users to buffer data in either a circular or linear fashion. Circular format (cir) is a revolving buffer file that is overwritten whenever the limit of the buffer size (set by `all.data_buffering`) is reached. In linear format (lin), data transmission between the remote device and the serial port ceases once the 4k bytes Rx buffer in the kernel is reached. Then if a session is established to the serial port, the data in the buffer is shown (`dont_show_DBmenu` must be 2), cleared, and data transmission is resumed. Linear buffering is impossible if flow control is set to none. Default is cir.

**Parameters Involved and Passed Values**

Data Buffering uses the following parameters:
**Data Buffering**

`all.data_buffering`  A non zero value activates data buffering (local or remote, according to what was configured in the parameter `conf.nfs_data_buffering`). If local data buffering, a file is created on the Cyclades-TS; if remote, a file is created through NFS in a remote server. All data received from the port is captured in this file. If local data buffering, this parameter means the maximum file size (in bytes). If remote, this parameter is just a flag to activate (greater than zero) or deactivate data buffering. When local data buffering is used, each time the maximum is reached the oldest 10% of stored data is discarded, releasing space for new data (FIFO system) - circular file. When remote data buffering is used, there’s no maximum file size other than the one imposed by the remote server - linear file. This file can be viewed using the normal UNIX tools (cat, vi, more, etc.). Size is in bytes not kilobytes.

`conf.nfs_data_buffering`  This is the Remote Network File System where data captured from the serial port will be written instead of being written to the local directory `/var/run/DB`. The directory tree to which the file will be written must be NFS-mounted, so the remote host must have NFS installed and the administrator must create, export and allow reading/writing to this directory. The size of this file is not limited by the value of the parameter `all.data_buffering`, though the value cannot be zero since a zero value turns off data buffering. The size of the file is dependent on the NFS server only (hard drive, partition size, etc.).
**Chapter 3 - Additional Features**

*all.DB_mode*  
When configured as cir for circular format, the buffer is like a revolving file that is overwritten whenever the limit of the buffer size (as configured in all.data_buffering or s<n>.data_buffering) is reached. When configured as lin for linear format, once 4k bytes of the Rx buffer in the kernel is reached, a flow control stop (RTS off or XOFF-depending on how all.flow or s<n>.flow is set) is issued to prevent the serial port from receiving further data from the remote. Then when a session is established to the serial port, a flow control start (RTS on or XON) will be issued and data reception will then resume. If all.flow or s<n>.flow is set to none, linear buffering isn’t possible. Default is cir.

*all.DB_user_logs*  
When "on", a line containing the time stamp, the username, the event itself (connection/disconnection) and the type of session (Read/Write or Read Only) will be added to the data buffering file every time a user connects or disconnected to the corresponding port.

The log message has the following formats :

1) "<connect> [timestamp] [username] [session type] </connect>
2) "<disconnect> [timestamp] [username] </disconnect>"

when [timestamp] = "YYYY-MM-DD hh:mm:ss"
[session type] = "Read/Write" or "Read Only"

*all.syslog_buffering*  
When nonzero, the contents of the data buffer are sent to the syslog-ng every time a quantity of data equal to this parameter is collected. The syslog level for data buffering is hard coded to level 5 (notice) and facility is local plus conf.DB_facility. The file /etc/syslog-ng/syslog-ng.conf should be set accordingly for the syslog-ng to take some action.
Data Buffering

all.syslog_sess
This parameter determines whether syslog is generated when a user is connected to the port or not. Originally, syslog is always generated whether the user is connected to the port or not. Now, users have the option to NOT have syslog generate messages when they connect to a port. This feature does not affect the local data_buffering file. When set to 0 (default), syslog is always generated. When set to 1, syslog is only generated when the user is NOT connected to the port sending the data. When the user does connect to the port that is sending data, syslog messages won't be generated.

all.dont_show_DBmenu
When zero, a menu with data buffering options is shown when a nonempty data buffering file is found. When 1, the data buffering menu is not shown. When 2, the data buffering menu is not shown but the data buffering file is shown if not empty. When 3, the data buffering menu is shown, but without the erase and show and erase options.

all.DB_timestamp
Records the time stamp in the data buffering file (1) or not (0). If it is configured as 1, the software will accumulate input characters until it receives a CR and LF from the serial port or the accumulated data reaches 256 characters. Either way, the accumulated data will be recorded in the data buffering file along with the current time. The parameter all.data_buffering has to be with a non-zero value for this parameter to be meaningful.

Configuration for CAS

vi Method
Files to be modified:
- pslave.conf
- syslog-ng.conf

Browser Method
To configure Data Buffering with your browser:
Chapter 3 - Additional Features

Step 1: **Point your browser to the Console Server.**
In the address or location field of your browser type the Console Access Server's IP address. For example:

http://10.0.0.0

Step 2: **Log in as root and type the Web root password configured by the Web server.**
This will take you to the Configuration and Administration page.

Step 3: **Select the Serial Ports link.**
Click on the Serial Ports link on the Link Panel to the left of the page or in the Configuration section of the page. This will take you to the Port Selection page.

Step 4: **Select port(s).**
On the Port Selection page, choose all ports or an individual port to configure, from the dropdown menu. Click the Submit button. This will take you to the Serial Port Configuration page.

Step 5: **Scroll down to the Data Buffering section.**
You can change the settings in this section.

<table>
<thead>
<tr>
<th>Data Buffering</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum Buffer Size (0-disabled): 0</td>
</tr>
<tr>
<td>Data Buffering Mode:</td>
</tr>
<tr>
<td>Data Buffer User Connection Log:</td>
</tr>
<tr>
<td>Records the Time Stamp in the Data Buffering File:</td>
</tr>
<tr>
<td>Buffer Size to Send Syslog (40 to 255, 0-disabled): 0</td>
</tr>
<tr>
<td>Syslog Buffering at All Times:</td>
</tr>
<tr>
<td>Data Buffering Menu:</td>
</tr>
<tr>
<td>Alarm for Data Buffering:</td>
</tr>
</tbody>
</table>

*Figure 25: Data Buffering section of the Serial Port Configuration page*

Step 6: **Click the Submit button.**

Step 7: **Select the General link.**
Click on the General link on the Link Panel to the left of the page.
Step 8: **Scroll down to the Data Buffering section.**

Choose whether NFS will be used or not, and choose the Data Buffering Facility level here.

![Data Buffering section of the General page](image)

*Figure 26: Data Buffering section of the General page*

Step 9: **Click the Submit button.**

Step 10: **Make the changes effective.**

Click on the Administration > Run Configuration link, check the Serial Ports/Ethernet/Static Routes box and click on the Activate Configuration button.

Step 11: **Click on the link Administration > Load/Save Configuration.**

Step 12: **Click the Save Configuration to Flash button.**

**Wizard Method**

Step 1: **Bring up the wizard.**

At the command prompt, type the following to bring up the Data Buffer custom wizard:

```
wiz --db
```

*Screen 1:*

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

Cyclades-TS
INSTRUCTIONS for using the Wizard:
You can:
1) Enter the appropriate information for your system and press ENTER. Enter '#' if you want to deactivate that parameter 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...

Screen 2:

***********************************************************
********* C O N F I G U R A T I O N   W I Z A R D *********
***********************************************************

Current configuration:
(The ones with the '#' means it's not activated.)

conf.nfs_data_buffering : #
all.data_buffering : 0
all.DB_mode : cir
all.dont_show_DBmenu : 0
all.DB_timestamp : 0
all.syslog_buffering : 0
all.syslog_sess : 0

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

Screen 3:

***********************************************************
********* C O N F I G U R A T I O N   W I Z A R D *********
***********************************************************
CONF.NFS_DATA_BUFFERING - This parameter applies only if users choose to remotely buffer data. This is the remote directory name where data buffering will be written to instead of the default directory '/var/run'. If deactivated, data buffering will be done locally.

conf.nfs_data_buffering[#] :

ALL.DATA_BUFFERING - For local data buffering, this parameter represents the maximum file size in bytes allowed to be captured before it is discarded for new space. If remote this parameter is just a flag to either activate (any value greater than 0) or deactivate data buffering.

all.data_buffering[0] :

Screen 4:

***********************************************************
********* C O N F I G U R A T I O N   W I Z A R D ***********
***********************************************************

ALL.DB_MODE - For local data buffering, this parameter allow users to buffer data in either a circular or linear fashion. Circular format (cir) is a revolving buffer file that is overwritten whenever the limit of the buffer size (set by all.data_buffering) is reached. In linear format (lin), data transmission between the remote device and the serial port ceases once the 4k bytes Rx buffer in the kernel is reached. Then if a session is established to the serial port, the data in the buffer is shown (dont_show_DBmenu must be 2), cleared, and data transmission is resumed. Linear buffering is impossible if flow control is set to none. Default is cir.

all.DB_mode[cir] :

ALL.DONT_SHOW_DBMENU - When 0, a menu with data buffering options is shown when a non-empty data buffering file is found. When 1, the data buffering menu is not shown. When 2, the data buffering menu is
not shown but the data buffering file is shown if not empty. When 3, the data buffering menu is shown, but without the 'erase and show' and 'erase' options.

all.dont_show_DBmenu[0] :

Screen 5:

***********************************************************
********* C O N F I G U R A T I O N W I Z A R D ***********
***********************************************************

ALL.DB_TIMESTAMP - Records the time stamp in the data buffering file (1) or not (0). In case it is configured as 1, the software will accumulate input characters until it receives a CR and LF from the serial port, or the accumulated data reaches 256 characters. Either way, the accumulated data will be recorded in the data buffering file along with the current time. The parameter, all.data_buffering, has to be nonzero in order for this parameter to work.

all.DB_timestamp[0] :

ALL.SYSLOG_BUFFERING - This parameter is another option to data buffering. Users can also have syslog perform this function along with data buffering into files. When nonzero, the contents of the data buffer are sent to the syslog-ng every time a quantity of data equal to this parameter is collected. The syslog level for data buffering is hard coded to level 5 (notice) and facility conf.DB_facility. The file /etc/syslog-ng/syslog-ng.conf should be set accordingly for the syslog-ng to take some action.

(Please see the 'Syslog-ng Configuration to use with Syslog Buffering Feature' section under Generating Alarms in Chapter 3 of the system's manual for the syslog-ng configuration file.)
all.syslog_buffering[0] :

Screen 6:

**********************************************************************************************
********** CONFIGURATION WIZARD **********
**********************************************************************************************

ALL.SYSLOG_SESS - In order for this parameter to function, make sure syslog buffering is activate. When set as 0, syslog messages are always generated whether or not there is a connection to the port that is sending data to your unit. When set to 1, syslog messages are NOT generated when there IS a connection to the port that is sending data. It is only generated when there isn't a session to the port that is sending data to your unit.

all.syslog_sess[0] :

Screen 7:

**********************************************************************************************
********** CONFIGURATION WIZARD **********
**********************************************************************************************

Current configuration:
(The ones with the '#' means it's not activated.)

conf.nfs_data_buffering : #
all.data_buffering : 0
all.DB_mode : cir
all.dont_show_DBmenu : 0
all.DB_timestamp : 0
all.syslog_buffering : 0
all.syslog_sess : 0

Are these configuration(s) all correct? (y/n) [n] :

If you type 'n'
Chapter 3 - Additional Features

Type 'c' to go back and CORRECT these parameters or 'q' to QUIT :

Typing 'c' repeats the application, typing 'q' exits the entire wiz application

If you type 'y'

Discard previous port-specific parameters? (y/n) [n] :

Note: Answering yes to this question will discard only the parameter(s) which you are currently configuring if they were configured for a specific port in a previous session. For instance, if you are currently configuring parameter, all.x, and there was a specific port, s2.x, configured; then, answering yes to this question will discard s2.x.

Type 'c' to CONTINUE to set these parameters for specific ports or 'q' to QUIT :

Typing 'c' leads to Screen 8, typing 'q' leads to Screen 9.

Screen 8:

******************************************************
********* C O N F I G U R A T I O N W I Z A R D *********
******************************************************
You have 8 available ports on this system.

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

Note: The number of available ports depends on the system you are on. Typing in a valid port number repeats this program except this time it's configuring for the port number you have chosen. Typing 'q' leads to Screen 9.
Data Buffering

*Screen 9:*

***********************************************************
********* C O N F I G U R A T I O N    W I Z A R D **********
***********************************************************

(Note: If you are NOT connected to this unit through a console, and you have just reconfigured the IP of this unit, activating the new configurations may cause you to lose connection. In that case, please reconnect to the unit by the new IP address, and manually issue a saveconf to save your configurations to flash.)

Do you want to activate your configurations now? (y/n) [y] :

*Screen 10:*

***********************************************************
********* C O N F I G U R A T I O N    W I Z A R D **********
***********************************************************

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.

If you choose to save to flash, your configurations thus far will still be in the memory of the system even after you reboot it. If you don't save to flash and if you were to reboot the system, all your new configurations will be lost and you will have to reconfigure the system.

Do you want to save your configurations to flash? (y/n) [n] :

**CLI Method**

To configure certain parameters for a specific serial port.
Chapter 3 - Additional Features

Step 1: At the command prompt, type in the appropriate command to configure desired parameters.

To activate the serial port. <string> should be ttyS<serial port number>:

```shell
config configure line <serial port number> tty <string>
```

To configure nfs_data_buffering:

```shell
config configure conf nfsdb <string>
```

To configure data_buffering:

```shell
config configure line <serial port number> databuffering <number>
```

To configure DB_mode:

```shell
config configure line <serial port number> dbmode <string>
```

To configure dont_show_DBmenu:

```shell
config configure line <serial port number> dbmenu <number>
```

To configure DB_timestamp:

```shell
config configure line <serial port number> dbtimestamp <number>
```

To configure syslog_buffering:

```shell
config configure line <serial port number> syslogdb <number>
```

Tip. You can configure all the parameters for a serial port in one line:

```shell
config configure line <serial port number> tty <string> conf nfsdb <string> db <number> dbmode <string> dbmenu <number> dbtimestamp <number> syslogdb <number>
```

Step 2: Activate and Save.
To activate your new configurations and save them to flash, type:

`config write`

(This is essentially typing `signal_ras bup` and `saveconf` from the normal terminal prompt.)
The DHCP (Dynamic Host Configuration Protocol) Client is available for firmware versions 1.2.x and above. DHCP is a protocol that allows network administrators to assign IP addresses automatically to network devices. Without DHCP (or a similar protocol like BOOTP), each device would have to be manually configured. DHCP automatically sends a new IP address to a connected device when it is moved to another location on the network. DHCP uses the concept of a fixed time period during which the assigned IP address is valid for the device it was assigned for. This “lease” time can vary for each device. A short lease time can be used when there are more devices than available IP numbers. For more information, see RFC 2131.

Parameter Involved and Passed Values

The DHCP client on the Ethernet Interface can be configured in two different ways, depending on the action the Cyclades-TS should take in case the DHCP Server does not answer the IP address request:

1. No action is taken and no IP address is assigned to the Ethernet Interface (most common configuration):
   - Set the global parameter conf.dhcp_client to 1.
   - Comment all other parameters related to the Ethernet Interface (conf.eth_ip, etc.).
   - Add the necessary options to the file /etc/network/dhcpcd_cmd (some options are described below).

2. The Cyclades-TS restores the last IP address previously provided in another boot and assigns this IP address to the Ethernet Interface. For the very first time the unit is powered ON, the IP address restored is 192.168.160.10 in case of failure in the DHCP. The unit goes out from the factory with DHCP enabled (conf.dhcp_client 2):
   - Set the global parameter conf.dhcp_client to 2.
   - Comment all other parameters related to the Ethernet Interface (conf.eth_ip, etc.).
   - Add the following lines to the file /etc/config_files:

   ```
   /etc/network/dhcpcd_cmd
   (from factory file already present in /etc/config_files)
   ```
/etc/dhcpcd-eth0.save
(From the factory, the file is already present in /etc/config_files.)

- Add the option “-x” to the factory default content of the file /etc/network/dhcpcd_cmd:

/sbin/dhcpcd -l 3600 -x -c /sbin/handle_dhcp
From the factory, /etc/network/dhcpcd_cmd already has such content.

- Add all other necessary options to the file /etc/network/dhcpcd_cmd (some options are described below). In both cases if the IP address of the Cyclades-TS or the default gateway are changed, the Cyclades-TS will adjust the routing table accordingly.

Two files are related to DHCP:

/bin/handle_dhcp The script which is run by the DHCP client each time an IP address negotiation takes place.

/etc/network/dhcpcd_cmd Contains a command that activates the DHCP client (used by the cy_ras program). Its factory contents are:

/bin/dhcpcd -c /bin/handle_dhcp

The options available that can be used on this command line are:

-D This option forces dhcpcd to set the domain name of the host to the domain name parameter sent by the DHCP Server. The default option is to NOT set the domain name of the host to the domain name parameter sent by the DHCP Server.

-H This option forces dhcpcd to set the host name of the host to the hostname parameter sent by the DHCP Server. The default option is to NOT set the host name of the host to the hostname parameter sent by the DHCP Server.

-R This option prevents dhcpcd from replacing the existing /etc/resolv.conf file.
Configuration for CAS, TS, and Dial-in Access

**vi Method**

Steps 1 and 2 under Parameters and Passed Values should be followed. You’ll need to edit /etc/portslave/pslave.conf, comment some lines, etc.

**Browser Method**

To configure DHCP via your Web browser:

**Step 1: Point your browser to the Console Server.**

In the address or location field of your browser type the Console Access Server’s IP address. For example:

http://10.0.0.0

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

This will take you to the Configuration and Administration page.

**Step 3: Click the General link on the Link Panel.**

This takes you to the General page.

**Step 4: Scroll down to the Ethernet port section.**

You can choose the DHCP Client option in this section. Select the radio button and click the Submit button at the bottom of the page.

**Note.** Do not modify the -c /bin/handle_dhcp option.
Step 5: **Make the changes effective.**

Click on the Administration > Run Configuration link, check the Serial Ports/Ethernet/Static Routes box and click on the Activate Configuration button.

Step 6: **Click on the link Administration > Load/Save Configuration.**

Step 7: **Click the Save Configuration to Flash button.**

The configuration will be saved in flash.
Chapter 3 - Additional Features

Filters

This feature is only available for firmware versions 1.2.x and above.

Description

The Cyclades-TS uses the Linux utility *ipchains* to filter IP packets entering, leaving and passing through its interfaces.

An ipchains tutorial is beyond the scope of this manual. For more information on ipchains, see the ipchains man page (not included with the Cyclades-TS).

The syntax of the ipchains command is:

```
ipchains -command chain rule-specification [options]
```

```
ipchains -E old-chain-name new-chain-name
```

where:

* chain is one of the following:

  * **input** Filters for packets coming into the Cyclades-TS itself.
  * **output** Filters for locally-generated packets.
  * **forward** Filters for packets being routed through the Cyclades-TS.
  * **user_created_chain** A previously defined (or in the process of being defined) chain created by the command “-N.”

* command:

  Only one command can be specified on the command line unless otherwise specified below. For all the long versions of the command and option names, you need to use only enough letters to ensure that ipchains can differentiate it from all other options.
Filters

Configuration for CAS, TS, and Dial-in Access

Browser Method
To configure filters in IP chains via your Web browser:

**Step 1:** Point your browser to the Cyclades-TS.

In the address or location field of your browser type:

<Console Access Server’s IP address>

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

This will take you to the Configuration and Administration page. (See “Configuration & Administration Menu page” on page 49)

**Step 3:** Click IPChains filter link.

Click on this link on the Link Panel. The following page will appear:

*Figure 28: IP Chain filtering*

**Step 4:** To create a new filter chain:

Type in the name of the filter chain in the Name box to the far right of the page, and then click the Add chain button. To enter the default target, click the appropriate Select button and then the Submit button. The new filter chain will be added to the Filter Chain Table.
Step 5: To edit or delete a filter chain:
   To change the default target or to delete the filter chain, click the radio button of the filter chain and then click the Edit chain button or the Delete chain button.

Step 6: To edit the rules of the filter chain:
   Click the radio button of the filter chain and then click the List rules button. If the filter chain doesn't have rules, you need to add them. Skip to Step 9.

Step 7: To delete a rule:
   Click the radio button of the rule and then click the Delete rule button.

Step 8: To edit a rule:
   Click the radio button of the rule and then click the Edit rule button.
Generating Alarms

This feature helps the administrator to manage the servers. It filters the messages received by the serial port (the server’s console) based on the contents of the messages. It then performs an action, such as sending an email or pager message. To configure this feature, you need to configure filters and actions in the syslog-ng.conf file. (You can read more about syslog-ng in the Syslog section.)

Port Slave Parameters Involved with Generating Alarms

conf_DB_facility  This value (0-7) is the Local facility sent to the syslog-ng with data when syslog_buffering and/or alarm is active.

all.alarm  When nonzero, all data received from the port is captured and sent to syslog-ng with INFO level and LOCAL[0+conf.DB_facility] facility.

Configuration for CAS, TS, and Dial-in Access

vi Method
Files to be modified:
- pslave.conf
- syslog-ng.conf

Browser Method
To configure PortSlave parameters involved with syslog-ng and the syslog-ng configuration file with your browser:

Step 1:  Point your browser to the Console Server.
In the address or location field of your browser type the Console Access Server’s IP address. For example:

http://10.0.0.0

Step 2:  Log in as root and type the Web root password configured by the Web server.
This will take you to the Configuration and Administration page.
Chapter 3 - Additional Features

Step 3: Select the General link.
Click on the General link on the Link Panel to the left of the page in the Configuration section. This will take you to the General page.

Step 4: Scroll down to the Data Buffering section.
You can change the Data Buffering Facility value (conf.DB_facility). Click the Submit button.

Step 5: Select the Serial Ports link.
Click on the Serial Ports link on the Link Panel to the left of the page in the Configuration section. This will take you to the Port Selection page.

Step 6: Select port(s).
On the Port Selection page, choose all ports or an individual port to configure from the dropdown menu. Click the Submit button. This will take you to the Serial Port Configuration page.

Step 7: Scroll down to the Data Buffering section.
You can change the “Alarm for Data Buffering” (.alarm) value. Click the Submit button.

Step 8: Select the Syslog link.
Click on the Syslog link on the Link Panel to the left of the page in the Configuration section. This will take you to the Edit the Syslog-ng Configuration File page.

Step 9: Make the changes effective.
Click on the Administration > Run Configuration link, check the Serial Ports/Ethernet/Static Routes box and click on the Activate Configuration button.

Step 10: Click on the link Administration > Load/Save Configuration.

Step 11: Click the Save Configuration to Flash button.
The configuration was saved in flash.
Generating Alarms

Wizard Method

The Alarm Generation custom wizard configures the ALL.ALARM parameter.

Step 1: Bring up the wizard.

At the command prompt, type the following to bring up the Alarm Generation custom wizard:

    wiz --al

Screen 1 (below) will appear.

Screen 1:

***********************************************************
********* C O N F I G U R A T I O N   W I Z A R D ***********
***********************************************************

ALL.ALARM - When non zero, all data received from the port are captured and sent to syslog-ng with INFO level and LOCAL[0+conf.DB_facility] facility. The syslog-ng.conf file should be set accordingly, for the syslog-ng to take some action.

(Please see the 'Syslog-ng Configuration to use with Alarm Feature' section under Generating Alarms in Chapter 3 of the system's manual for the syslog-ng configuration file.)

all.alarm[0]:

---

Cyclades-TS
Screen 2:

***********************************************************
********* C O N F I G U R A T I O N W I Z A R D *********
***********************************************************

Current configuration:
(The ones with the '#' means it's not activated.)

all.alarm : 0

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

Screen 3:

***********************************************************
********* C O N F I G U R A T I O N W I Z A R D *********
***********************************************************

ALL.ALARM - When non zero, all data received from the port are captured and sent to syslog-ng with DAEMON facility and ALERT level. The syslog-ng.conf file should be set accordingly, for the syslog-ng to take some action. (Please see the 'Syslog-ng Configuration to use with Alarm Feature' section under Generating Alarms in Chapter 3 of the system's manual for the syslog-ng configuration file.)

all.alarm[0] :

Note: conf.DB_facility is configured under the syslog parameters (wiz --sl).
Generating Alarms

Screen 4:

**********************************************************************
******* CONFIGURATION WIZARD **********
**********************************************************************
Current configuration:
(The ones with the '#' means it's not activated.)

all.alarm : 0

Are these configuration(s) all correct? (y/n) [n] :

If you type 'n'

Type 'c' to go back and CORRECT these parameters or 'q' to QUIT :

Typing 'c' repeats the application, typing 'q' exits the entire wiz application

If you type 'y'

Discard previous port-specific parameters? (y/n) [n] :

Note: Answering yes to this question will discard only the parameter(s) which you are currently configuring if they were configured for a specific port in a previous session. For instance, if you are currently configuring parameter, all.x, and there was a specific port, s2.x, configured; then, answering yes to this question will discard s2.x.

Type 'c' to CONTINUE to set these parameters for specific ports or 'q' to QUIT :

Typing 'c' leads to Screen 5, typing 'q' leads to Screen 6.
Chapter 3 - Additional Features

Screen 5:
***********************************************************
********* C O N F I G U R A T I O N W I Z A R D ***********
***********************************************************

You have 8 available ports on this system.

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

Note: The number of available ports depends on the system you are on. Typing in a valid port number repeats this program except this time it's configuring for the port number you have chosen. Typing 'q' leads to Screen 6.

Screen 6:
***********************************************************
********* C O N F I G U R A T I O N W I Z A R D ***********
***********************************************************

(Note: If you are NOT connected to this unit through a console, and you have just reconfigured the IP of this unit, activating the new configurations may cause you to lose connection. In that case, please reconnect to the unit by the new IP address, and manually issue a saveconf to save your configurations to flash.)

Do you want to activate your configurations now? (y/n) [y] :
Generating Alarms

Screen 7:
***********************************************************
********* CONFIGURATION WIZARD ***********
***********************************************************

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.

If you choose to save to flash, your configurations thus far will still be in the memory of the system even after you reboot it. If you don't save to flash and if you were to reboot the system, all your new configurations will be lost and you will have to reconfigure the system.

Do you want to save your configurations to flash? (y/n) [n] :

CLI Method
To configure certain parameters for a specific serial port:

Step 1: At the command prompt, type in the appropriate command to configure desired parameters.

To activate the serial port. <string> should be ttyS<serial port number> :

config configure line <serial port number> tty <string>

To configure conf.DB_facility:

config configure conf dbfacility <number>

To configure alarm:

config configure line <serial port number> alarm <number>

Tip. You can configure all the parameters for a serial port in one line.

config configure line <serial port number> tty <string> alarm <number>
Chapter 3 - Additional Features

Step 2: Activate and Save.
To activate your new configurations and save them to flash, type:

```
config write
```

(This is essentially typing `signal_ras hup` and `saveconf` from the normal terminal prompt.)

Syslog-ng Configuration to use with Alarm Feature
This configuration example is used for the alarm feature.

Step 1: Configure the pslave.conf file parameter.
In the pslave.conf file the parameters of the alarm feature are configured as:

```
all.alarm 1
conf.DB_facility 2
```

Step 2: Add lines to syslog-ng.conf.
The syslog-ng.conf file needs these lines:

```
# local syslog clients
source sysl { unix-stream("/dev/log"); };

# To filter ALARM message with the string "kernel panic" :
filter f_kpanic { facility(local2) and level(info) and match("ALARM") and match("kernel panic"); };

# To filter ALARM message with the string "root login" :
filter f_root { facility(local2) and level(info) and match("ALARM") and match("root login"); };

# To send e-mail to z@none.com (SMTP's IP address 10.0.0.2)
# from the e-mail address a@none.com with subject "ALARM".
# The message will carry the current date, the hostname
```
Generating Alarms

# of this unit and the message that was received from the source.

destination d_mail1 {
    pipe("/dev/cyc_alarm"
        template("sendmail -t z@none.com -f a@none.com -s "ALARM" -m "$FULLDATE $HOST $MSG" -h 10.0.0.2"));
    }

# Example to send a pager to phone number 123 (Pager server at 10.0.0.1) with message
# carrying the current date, the hostname of this TS and the message that was received from the source :

destination d_pager {
    pipe("/dev/cyc_alarm"
        template("sendsms -d 123 -m "$FULLDATE $HOST $MSG" 10.0.0.1"));
    }

# Example to send a Link Down trap to server at 10.0.0.1 with message carrying the current date, the hostname of this unit and the message that received from the source :

destination d_trap {
    pipe("/dev/cyc_alarm"
        template("snmptrap -v1 10.0.0.1 public "$" "$" 2 0 "$" \.1.3.6.1.2.1.2.1.2.1.2.1 s "$FULLDATE $HOST $MSG" ");
    }

# To send e-mail and snmptrap if message received from local syslog client has the string "kernel panic" :
Chapter 3 - Additional Features

log { source(sysl); filter(f_kpanic); destination(d_mail1); destination(d_trap); };

# To send e-mail and pager if message received from local syslog client has the string
# "root login":
log { source(sysl); filter(f_root); destination(d_mail1); destination(d_pager); }

Alarm, Sendmail, Sendsms and Snmptrap

Alarm
This feature is available only for the Console Server Application. The TS sends messages using pager, e-mail, or snmptrap if the serial port receives messages with specific string. To configure this feature:

Step 1: Activate alarm in Portslave configuration file.
Parameter all.alarm - 0 inactive or <> 0 active.

Step 2: Configure filters in the syslog-ng configuration file.

filter f_alarm { facility(local[0+conf.DB_facility]) and level(info) and match("ALARM") and match("<your string>"); }

Example: to filter the ALARM message with the string “kernel panic” (conf.DB_facility is configured with value 1):

filter f_kpanic { facility(local1) and level(info) and match("ALARM") and match("kernel panic"); }

Example: to filter the ALARM message with the string “root login”:

filter f_root { facility(local1) and level(info) and match("ALARM") and match("root login"); }

Step 3: Configure actions in the syslog-ng configuration file.
(See more details in syslog-ng examples.)

Example: alarm is active and if the serial port receives the string “kernel panic,” one message will be sent to the pager.
Generating Alarms

log (source(sysl); filter(f_kpanic); destination(d_pager); );

To send e-mail:

destination d_mail { pipe("/dev/cyc_alarm" template("sendmail <pars>") ); };

To send a pager message:

destination d_pager { pipe("/dev/cyc_alarm" template("sendsms <pars>") ); };

To send snmptrap:

destination d_trap { pipe("/dev/cyc_alarm" template("snmptrap <pars>") ); };

Step 4: Connect filters and actions in the syslog-ng configuration file.

Example: alarm is active and if the serial port receives the string “kernel panic,” one message will be sent to the pager.

log (source(sysl); filter(f_kpanic); destination(d_trap); destination(d_pager); );

Sendmail

Sendmail sends a message to a SMTP server. It is not intended as a user interface routine; it is used only to send pre-formatted messages. Sendmail reads all parameters in the command line. If the SMTP server does not answer the SMTP protocol requests sent by sendmail, the message is dropped.
Chapter 3 - Additional Features

Synopsis:

sendmail -t <name>[,<name>] [-c <name> [,<name>]] [-b <name> [,<name>]] [-r <name>] -f <name> -s <text> -m <text> -h <SMTP server> [-p <smtp-port>]

where:

- **-t <name>[,<name>]**  
  “To: ” Required. Multi-part allowed (multiple names are separated by commas). Names are expanded as explained below.

- **[-c <name> [,<name>]]**  
  “Cc: ” Optional. Multi-part allowed (multiple names are separated by commas).

- **[-b <name> [,<name>]]**  
  “Bcc: ” Optional. Multi-part allowed (multiple names are separated by commas).

- **[-r <name>]**  
  “Reply-To: ” Optional. Use the Reply-To: field to make sure the destination user can send a reply to a regular mailbox.

- **-f <name>**  
  “From: ” Required.

- **-s <text>**  
  "Subject: " Required.

- **-m <text>**  
  "body" The message body.

- **-h <SMTP server>**  
  Required. IP address or name of the SMTP server.

- **[-p <SMTP port>]**  
  Optional. The port number used in the connection with the server. Default: 25.

- **<name>**  
  Any email address.

- **<text>**  
  A text field. As this kind of field can contain blank spaces, please use the quotation marks to enclose the text.

For example, to send e-mail to z@none.com (SMTP's IP address 10.0.0.2) from the e-mail address a@none.com with subject “sendmail test.”

sendmail -t z@none.com -f a@none.com -s "sendmail test" -m "Send-mail test. \n Is it OK???
 " -h 10.0.0.2
**Generating Alarms**

Sendsms
The sendsms is the Linux command line client for the SMSLink project. It accepts command line parameters that define the message to be sent, and transmits them to the SMS server process running on the designated server. The sendsms was developed specifically for easy calling from shell scripts or similar situations.

**Synopsis:**

```
sendsms [-r] [-g] [-v] -d dest (-m message or -f msgfile)
[-u user] [-p port] server
```

where:

- **-r** Reporting. Additional info will be included in the message printed on stderr (namely, the device name used by the server to send the SMS out, and the message ID attributed to the SMS by the module's SIM card). If any of these items is missing or can't be parsed, a value of "??" will be returned.

- **-g** Turns debugging on. Will output the entire dialog with the server on stderr (and more).

- **-h** Displays a short help message and exits.

- **-v** Displays version information and exits.

- **-d dest** Required. The GSM network address (i.e. phone number) of the mobile phone the message is to be sent to. Supported format is: [int. prefix - country code] area code - phone number. The international prefix can be either "+" or "00" (or any other value supported by the GSM network provider the server is subscribed to). Some separation characters can be used to beautify the number, but they are purely cosmetic and will be stripped by the server. Those characters are [./- ]. The pause character (',') is not supported. Regarding the international country code, don't forget that its necessity is to be considered respective to the SMS gateway location (the host this client program is connecting to), not the location where the client is run from.
Chapter 3 - Additional Features

- **d dest (cont.)**
  If there are any doubts, please contact the SMS server administrator for your network. Please always include the area code (even when sending to a destination in the same “area”, i.e., on the same network). The number without the area code, though syntactically correct and accepted by the network, may never get delivered.

- **m message**
  Required (Use one and only one of “-m” or “-f”). The text of the message to be sent. Unless made up of a single word, it will have to be quoted for obvious reasons. Maximum length is 160 characters. A longer message will be truncated (you will be warned about it), but the message will still be sent. At the present time, only 7-bit ASCII is supported for the message text.

- **f msgfile**
  Required (use one and only one of “-m” or “-f”). The name of a text file where the message to send is to be read from. This file can contain multiple lines of text (they will be concatenated), but its total length can’t exceed 160 characters. A longer text will be truncated (you will be warned about it), but the message will still be sent. The special file ‘-‘ means that input will be read from stdin. At the present time, only 7-bit ASCII is supported for the message text.

- **u user**
  Optional. The server module requires the user to identify her/himself for logging purposes. No authentication is performed on this information, however. If this parameter is omitted, sendsms will send the UNIX username of the current user. This parameter allows you to override this default behavior (might be useful in the case of automated sending).

- **p port**
  Optional. Communication port on the target server. If provided here, this value will be used to connect to the server. If omitted, the client will query the local system for the port number associated with the “well known service” sms (as defined in /etc/services). If that doesn’t return an answer, the compiled-in default value 6701 will be used.
Example to send a pager message to phone number 123 (Pager server at 10.0.0.1) with message:

```
sendsms -d 123 -m "Hi. This is a test message send from TS using sendsms" 10.0.0.1
```

### Snmptrap

Snmptrap is an SNMP application that uses the TRAP-PDU Request to send information to a network manager. One or more fully qualified object identifiers can be given as arguments on the command line. A type and a value must accompany each object identifier. Each variable name is given in the format specified. If any of the required version 1 parameters—enterprise-oid, agent and uptime—are specified as empty, it defaults to “.1.3.6.1.4.1.3.1.1”, hostname, and host-uptime respectively.

### Synopsis

```
snmptrap -v 1 [-Ci] [common arguments] enterprise-oid agent generic-trap specific-trap uptime [objectId type value]...
```

```
snmptrap -v [2c|3] [-Ci] [common arguments] uptime trap-oid [objectId type value]...
```
where:

-\textit{Ci} Optional. It sends INFORM-PDU.

\textbf{common arguments} Required. They are:
"-c <community name> <SNMP server IP address>"

\textbf{enterprise-oid} Required, but it can be empty (".").

\textbf{agent} Required, but it can be empty ("). The agent name.

\textbf{generic-trap} The generic trap number: 2 (link down), 3 (link up), 4 (authentication failure), ...

\textbf{specific-trap} Required. The specific trap number.

\textbf{uptime} Required.

\textbf{[objectID type value]} Optional. objectID is the object oid. You want to inform its value to server.

If the network entity has an error processing the request packet, an error packet will be returned and a message will be shown, helping to pinpoint in what way the request was malformed. If there were other variables in the request, the request will be resent without the bad variable.

For example, to send a Link Down trap to server at 10.0.0.1 with interfaces.iftable.ifentry.ifde-scr:

\texttt{snmptrap -v 1 10.0.0.1 public "" 2 0 "" .1.3.6.1.2.1.2.2.1.2.1 s "TS: serial port number 1 is down"}

-\textit{Ci} Optional. It sends INFORM-PDU.

\textbf{common arguments} Required. They are: SNMP server IP address and community.

\textbf{enterprise-oid} Required, but it can be empty (".)
Help Wizard Information

Synopsis: wiz [--OPTIONS] [--port <port number>]

Note: To directly configure a feature for a specific serial port, use the "--port <port number>" option after "wiz - [option]."

Note: Make sure there are two hyphens before any of the options listed on the following table.

Table 10: General Options for the Help Wizard

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ac &lt;cas or ts&gt;</td>
<td>Configuration of access method parameters</td>
</tr>
<tr>
<td>al</td>
<td>Configuration of alarm parameter</td>
</tr>
<tr>
<td>all &lt;cas or ts&gt;</td>
<td>Configuration of all parameters</td>
</tr>
<tr>
<td>auth</td>
<td>Configuration of authentication parameters</td>
</tr>
<tr>
<td>db</td>
<td>Configuration of data buffering parameters</td>
</tr>
<tr>
<td>help</td>
<td>Print this help message</td>
</tr>
<tr>
<td>pm</td>
<td>Configuration of power management parameters.</td>
</tr>
</tbody>
</table>
Chapter 3 - Additional Features

Table 10: General Options for the Help Wizard

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sl</td>
<td>Configuration of syslog parameters</td>
</tr>
<tr>
<td>snf</td>
<td>Configuration of sniffing parameters</td>
</tr>
<tr>
<td>sset &lt;cas or ts&gt;</td>
<td>Configuration of serial setting parameters</td>
</tr>
<tr>
<td>tl</td>
<td>Configuration of terminal login display parameters</td>
</tr>
<tr>
<td>tso</td>
<td>Configuration of other parameters specific to the TS profile</td>
</tr>
</tbody>
</table>

Step 1: Bring up the wizard.
At the command prompt, type the following to bring up the Help custom wizard (you can also type wiz -h):

    wiz --help

Help Command Line Interface Information

Note: To enter into CLI mode, type config at the terminal prompt. You will then get a CLI prompt similar to config@hostname>>. Once in CLI mode, you eliminate the need to type config at the beginning of your CLI commands. To exit from this mode, type exit or quit.

Synopsis 1 - Configuration of Port Specific Parameters

    config configure line [serial port number] [options]

    or in CLI mode:

    configure line [serial port number] [options]

The following table shows Help CLI Options and the actual parameter modified for Synopsis 1.
Table 11: Help CLI Options - Synopsis 1

<table>
<thead>
<tr>
<th>Option</th>
<th>Actual Parameter Modified</th>
</tr>
</thead>
<tbody>
<tr>
<td>accthost1 &lt;string&gt;</td>
<td>accthost1</td>
</tr>
<tr>
<td>accthost2 &lt;string&gt;</td>
<td>accthost2</td>
</tr>
<tr>
<td>adminusers &lt;string&gt;</td>
<td>admin_users</td>
</tr>
<tr>
<td>alarm &lt;number&gt;</td>
<td>alarm</td>
</tr>
<tr>
<td>authhost1 &lt;string&gt;</td>
<td>authhost1</td>
</tr>
<tr>
<td>authhost2 &lt;string&gt;</td>
<td>authhost2</td>
</tr>
<tr>
<td>authtype &lt;string&gt;</td>
<td>authtype</td>
</tr>
<tr>
<td>auto_input &lt;string&gt;</td>
<td>auto_answer_input</td>
</tr>
<tr>
<td>auto_output &lt;string&gt;</td>
<td>auto_answer_output</td>
</tr>
<tr>
<td>break &lt;string&gt;</td>
<td>break_sequence</td>
</tr>
<tr>
<td>datasize &lt;number&gt;</td>
<td>datasize</td>
</tr>
<tr>
<td>databuffering &lt;number&gt;</td>
<td>data_buffering</td>
</tr>
<tr>
<td>dbmenu &lt;number&gt;</td>
<td>dont_show_DBmenu</td>
</tr>
<tr>
<td>dbmode &lt;string&gt;</td>
<td>DB_mode</td>
</tr>
<tr>
<td>dbtimestamp &lt;number&gt;</td>
<td>DB_timestamp</td>
</tr>
<tr>
<td>dcd &lt;number&gt;</td>
<td>dcd</td>
</tr>
<tr>
<td>dtr_reset &lt;number&gt;</td>
<td>DTR_reset</td>
</tr>
<tr>
<td>escape &lt;string&gt;</td>
<td>escape_char</td>
</tr>
<tr>
<td>flow &lt;string&gt;</td>
<td>flow</td>
</tr>
<tr>
<td>host &lt;string&gt;</td>
<td>host</td>
</tr>
<tr>
<td>idletimeout &lt;number&gt;</td>
<td>idletimeout</td>
</tr>
</tbody>
</table>
Table 11: Help CLI Options - Synopsis 1

<table>
<thead>
<tr>
<th>Option</th>
<th>Actual Parameter Modified</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipno &lt;string&gt;</td>
<td>ipno</td>
</tr>
<tr>
<td>issue &lt;string&gt;</td>
<td>issue</td>
</tr>
<tr>
<td>If &lt;number&gt;</td>
<td>If_suppress</td>
</tr>
<tr>
<td>modbus &lt;string&gt;</td>
<td>modbus_smode</td>
</tr>
<tr>
<td>multiplesess &lt;string&gt;</td>
<td>multiple_sessions</td>
</tr>
<tr>
<td>parity &lt;string&gt;</td>
<td>parity</td>
</tr>
<tr>
<td>pmkey &lt;string&gt;</td>
<td>pmkey</td>
</tr>
<tr>
<td>pmnumofoutlets &lt;number&gt;</td>
<td>pmNumOfOutlets</td>
</tr>
<tr>
<td>pmoutlet &lt;string&gt;</td>
<td>pmoutlet</td>
</tr>
<tr>
<td>pmttype &lt;string&gt;</td>
<td>pmttype</td>
</tr>
<tr>
<td>pmusers &lt;string&gt;</td>
<td>pmusers</td>
</tr>
<tr>
<td>pollinterval &lt;number&gt;</td>
<td>poll_interval</td>
</tr>
<tr>
<td>prompt &lt;string&gt;</td>
<td>prompt</td>
</tr>
<tr>
<td>protocol &lt;string&gt;</td>
<td>protocol</td>
</tr>
<tr>
<td>retries &lt;number&gt;</td>
<td>timeout</td>
</tr>
<tr>
<td>secret &lt;string&gt;</td>
<td>secret</td>
</tr>
<tr>
<td>sniffmode &lt;string&gt;</td>
<td>sniff_mode</td>
</tr>
<tr>
<td>socket &lt;number&gt;</td>
<td>socket_port</td>
</tr>
<tr>
<td>speed &lt;number&gt;</td>
<td>speed</td>
</tr>
<tr>
<td>stopbits &lt;number&gt;</td>
<td>stopbits</td>
</tr>
<tr>
<td>sttycmd &lt;string&gt;</td>
<td>sttyCmd</td>
</tr>
<tr>
<td>syslogdb &lt;number&gt;</td>
<td>syslog_buffering</td>
</tr>
</tbody>
</table>
Help

Table 11: Help CLI Options - Synopsis 1

<table>
<thead>
<tr>
<th>Option</th>
<th>Actual Parameter Modified</th>
</tr>
</thead>
<tbody>
<tr>
<td>syslogsess &lt;number&gt;</td>
<td>syslog_sess</td>
</tr>
<tr>
<td>telnetclientmode &lt;number&gt;</td>
<td>telnet_client_mode</td>
</tr>
<tr>
<td>term &lt;string&gt;</td>
<td>term</td>
</tr>
<tr>
<td>timeout &lt;number&gt;</td>
<td>timeout</td>
</tr>
<tr>
<td>tty &lt;string&gt;</td>
<td>tty</td>
</tr>
<tr>
<td>txinterval &lt;number&gt;</td>
<td>tx_interval</td>
</tr>
<tr>
<td>userauto &lt;string&gt;</td>
<td>userauto</td>
</tr>
<tr>
<td>users &lt;string&gt;</td>
<td>users</td>
</tr>
</tbody>
</table>

(Refer to Appendix C for more info on the parameters.)

Synopsis 2 - Configuration of Network-related Parameters

config configure ether [options]

or in CLI mode:

configure ether [options]

Table 12: Help CLI Options - Synopsis 2

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Actual Parameters Modified</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip &lt;string&gt;</td>
<td>Configuration of the IP of the Ethernet interface.</td>
<td>confeth_ip</td>
</tr>
<tr>
<td>mask &lt;string&gt;</td>
<td>Configuration of the mask for the Ethernet network.</td>
<td>confeth_mask</td>
</tr>
<tr>
<td>mtu &lt;number&gt;</td>
<td>Configuration of the Maximum Transmission Unit size.</td>
<td>confeth_mtu</td>
</tr>
</tbody>
</table>
Chapter 3 - Additional Features

(Refer to Appendix C for more info on the parameters.)

Synopsis 3 - Configuration of other Conf. Parameters

config configure conf [options]

or in CLI mode:

configure conf [options]

<table>
<thead>
<tr>
<th>Option</th>
<th>Actual Parameter Modified</th>
</tr>
</thead>
<tbody>
<tr>
<td>dbfacility &lt;number&gt;</td>
<td>conf.DB_facility</td>
</tr>
<tr>
<td>facility &lt;number&gt;</td>
<td>conf.facility</td>
</tr>
<tr>
<td>group &lt;string&gt;</td>
<td>conf.group</td>
</tr>
<tr>
<td>locallogins &lt;number&gt;</td>
<td>conf.locallogins</td>
</tr>
<tr>
<td>nfsdb &lt;string&gt;</td>
<td>conf.nfs_data_buffering</td>
</tr>
</tbody>
</table>

(Refer to Appendix C for more info on the parameters.)
To obtain general help on the format of CLI, type `config help | more` at the terminal prompt.

Help may be requested at any point in a command by entering a “?” If nothing matches, the help list will be empty and you must backup until entering a “?” shows the available options.

For example:

- To find out possible commands that can come after `config`, type:
  
  `config ?`

- To find out what parameters are configurable through CLI, type:
  
  `config configure line <serial port number> ?`

Note: To include spaces within the string you are configuring, encapsulate the string within single or double quotes. For instance, to configure s2.sttyCmd -igncr -onlcr, type (do not put a space after a comma):

```
config configure line 2 sttycmd "-igncr -onlcr"
```

Tip. You can specify the range or list of serial ports if you wish to configure the same parameters for several ports. For instance, to configure parameters for ports 2 through 4, you can type this command: `config configure line 2-4 [options]`. Or to configure parameters for just ports 4, 6, and 9, you can type:

```
config configure line 4,6,9 [options]
```

(Do not put a space after the commas when listing the serial ports.)
MODBUS is an application layer messaging protocol for client/server communication which is widely used in the industrial automation. It is a confirmed service protocol and offers many services specified by function codes, like reading and writing registers on PLCs.

A protocol converter for the MODBUS protocol over the TCP/IP communication stack (Modbus/TCP) is implemented in the Cyclades-TS and converts Modbus/TCP ADUs from the Ethernet interface to plain MODBUS message frames over a serial RS-232 or RS-485 interface, and vice versa, supporting both serial modes (ASCII and RTU).

Figure 29: Modbus application
In this example, the Automation Application running in the Workstation (local or remote) controls the PLCs connected to the serial port (RS-485) of the Cyclades-TS110/100 using MODBUS/TCP protocol. The connection is opened using the Cyclades-TS110/100 Ethernet IP address and TCP port = 502. The Cyclades-TS110/100 accepts the incoming connection and converts MODBUS/ TCP ADUs (packets) to plain MODBUS frames and sends them over the serial port. On the other hand, the MODBUS frames received from the serial port are converted to MODBUS/ TCP ADUs and sent through the TCP connection to the Automation Application.

The configuration described earlier for Console Access Servers (see Figure 1: Console Access Server diagram) should be followed with the following exceptions for this example:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Value for this Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>all.protocol</td>
<td>For the console server profile, the possible protocols are socket_server (when telnet is used), socket_ssh (when ssh version one or two is used), raw_data (to exchange data in transparent mode – similar to socket_server mode, but without telnet negotiation, breaks to serial ports, etc.), or modbus (an application layer messaging protocol for client/server communication widely used for industrial automation).</td>
<td>modbus</td>
</tr>
<tr>
<td>all.modbus_smode</td>
<td>Communication mode through the serial ports. This parameter is meaningful only when modbus protocol is configured. The valid options are ascii (normal TX/RX mode) and rtu (some time constraints are observed between characters while transmitting a frame). If not configured, ASCII mode will be assumed.</td>
<td>ascii</td>
</tr>
</tbody>
</table>
Chapter 3 - Additional Features

NTP

The ntpclient is a Network Time Protocol (RFC-1305) client for UNIX- and Linux-based computers. In order for the Cyclades-TS to work as a NTP client, the IP address of the NTP server must be set in the file /etc/ntpclient.conf.

The script shell /bin/daemon.sh reads the configuration file (/etc/ntpclient.conf) and build the line command to call /bin/ntpclient program.

Parameters Involved and Passed Values

The file /etc/ntpclient.conf has the value of two parameters:

- **ENABLE**
  This parameter enables the NTP client. It defaults to NO, to enable it choose “YES”.

- **NTPSERVER**
  The IP address of the NTP server.

- **NTPINTERVAL**
  Check time every interval seconds (default 300).

The data and time will be updated from the NTP server according to the parameter options. The ntpclient program has this syntax:

```plaintext
ntpclient [options]
```

**Options:**

- **-c count**
  Stop after count time measurements (default 0 means go forever).
- **-d**
  Print diagnostics.
- **-h hostname**
  NTP server host (mandatory).
- **-i interval**
  Check time every interval seconds.
- **-l**
  Attempt to lock local clock to server using adjtimex(2).
- **-p port**
  Local NTP client UDP port.
Configuration for CAS, TS, and Dial-in Access

**vi Method**

Files to be changed:

/etc/ntpclient.conf

**Browser Method**

To configure NTP with your browser:

**Step 1:** **Point your browser to the Console Server.**

In the address or location field of your browser type the Console Access Server’s IP address. For example:

http://10.0.0.0

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

This will take you to the Configuration and Administration page.

**Step 3:** **Click on the Edit Text File link.**

Click on this link on the Link Panel or on the Configuration section of the Configuration and Administration page. (See Figure 17: Configuration and Administration page.) You can then pull up the appropriate file and edit it.
Chapter 3 - Additional Features

Ports Configured as Terminal Servers

Important! TS110/100 owners: please skip to the special section on the TS110/100 later in the installation chapter called Configuring the Cyclades- 
TS110/100 for the first time, then perform “Task 5: Activate the changes” on 
page 69 through listed in Chapter 2 - Installation and Configuration to finish 
the configuration. Make into links.

There are TS-specific parameters that are required to be configured when using the serial 
ports with the TS profile. The configuration of these TS-specific parameters are described in 
this section. Additional configuration for TS is described in Access Method and Serial Settings 
in Chapter 3, and in Appendix C – The pslave Configuration File.

TS Setup Wizard

The Wizard can be used to configure TS-specific parameters. (TSO stands for “TS Other”- 
other parameters specific to the TS profile):

Step 1: At the command line interface type the following:

wiz --tso

Screen 1:

**************************************************************************************
************** CONFIGURATION WIZARD **************
**************************************************************************************

INSTRUCTIONS for using the Wizard:
You can:
1) Enter the appropriate information for your system
and press ENTER. Enter '#' if you want to
deactivate that parameter or
2) Press ENTER if you are satisfied with the value
within the brackets [ ] and want to go on to the
Ports Configured as Terminal Servers

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...

Screen 2:

***********************************************************
********* C O N F I G U R A T I O N   W I Z A R D ***********
***********************************************************

Current configuration:
(The ones with the '#' means it's not activated.)

all.host : 192.168.160.8
all.term : vt100
conf.locallogins : 0

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

Screen 3:

***********************************************************
********* C O N F I G U R A T I O N   W I Z A R D ***********
***********************************************************

ALL.HOST - The IP address of the host to which the
terminals will connect.

all.host[192.168.160.8] :

ALL.TERM - This parameter defines the terminal type assumed
when performing rlogin or telnet to other hosts.

all.term[vt100] :
Chapter 3 - Additional Features

Screen 4:

***********************************************************
********* Configuration Wizard *********
***********************************************************
CONF.LOCALLOGINS - This parameter is only necessary when authentication is being performed for a port. When set to 1, it is possible to log into the system directly by placing a '!' before users' login name, then using their normal password. This is useful if the Radius authentication server is down.

conf.locallogins[0] :

Screen 5:

***********************************************************
********* Configuration Wizard *********
***********************************************************
Current configuration:
(The ones with the '#' means it's not activated.)

all.host : 192.168.160.8
all.term : vt100
conf.locallogins : 0

Are these configuration(s) all correct? (y/n) [n] :

If you type 'n'
Type 'c' to go back and CORRECT these parameters or 'q' to QUIT :
Typing 'c' repeats the application, typing 'q' exits the entire wiz application

If you type 'y'
Discard previous port-specific parameters? (y/n) [n] :
Note: Answering yes to this question will discard only the parameter(s) which you are currently configuring if they were configured for a specific port in a previous session. For instance, if you are currently configuring parameter, all.x, and there was a specific port, s2.x, configured; then, answering yes to this question will discard s2.x.

Type 'c' to CONTINUE to set these parameters for specific ports or 'q' to QUIT:

Typing 'c' leads to Screen 6, typing 'q' leads to Screen 7.

Screen 6:

You have 8 available ports on this system.

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

Tip: The number of available ports depends on the system you are on. Typing in a valid port number repeats this program except this time it's configuring for the port number you have chosen. Typing 'q' leads to Screen 7.
Chapter 3 - Additional Features

Screen 7:

***********************************************************
********* CONFIGURATION WIZARD *********
***********************************************************

(Note: If you are NOT connected to this unit through a console, and you have just reconfigured the IP of this unit, activating the new configurations may cause you to lose connection. In that case, please reconnect to the unit by the new IP address, and manually issue a saveconf to save your configurations to flash.)

Do you want to activate your configurations now? (y/n) [n]:

Screen 8:

***********************************************************
********* CONFIGURATION WIZARD *********
***********************************************************

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.

If you choose to save to flash, your configurations thus far will still be in the memory of the system even after you reboot it. If you don't save to flash and if you were to reboot the system, all your new configurations will be lost and you will have to reconfigure the system.

Do you want to save your configurations to flash? (y/n) [n]:

User Guide 193
Ports Configured as Terminal Servers

CLI Method
To configure certain parameters for a specific serial port:

**Step 1:** At the command prompt, type in the appropriate command to **configure desired parameters**.

To activate the serial port. `<string>` should be `ttyS<serial port number>`:

```plaintext
config configure line <serial port number> tty <string>
```

To configure host:

```plaintext
config configure line <serial port number> host <string>
```

To configure term:

```plaintext
config configure line <serial port number> term <string>
```

To configure conf.locallogins:

```plaintext
config configure conf locallogins <number>
```

**Tip.** You can configure all the parameters for a serial port in one line.

```plaintext
config configure line <serial port number> tty <string> host <string> term <string> locallogins <number>
```

**Step 2:** **Activate and Save.**

To activate your new configurations and save them to flash, type:

```plaintext
config write
```

(This is essentially typing `signal_ras hap` and `saveconf` from the normal terminal prompt.)
Chapter 3 - Additional Features

Serial Settings

This feature controls the speed, data size, parity, and stop bits of all ports. It also sets the flow control to hardware, software, or none; the DCD signal; and tty settings after a socket connection to that serial port is established.

Parameters Involved and Passed Values

Terminal Settings involve the following parameters (the first four are physical parameters):

- **all.speed**
  - The speed for all ports. Default value: 9600.

- **all.datasize**
  - The data size for all ports. Default value: 8.

- **all.stopbits**
  - The number of stop bits for all ports. Default value: 1.

- **all.parity**
  - The parity for all ports. Default value: none.

- **all.flow**
  - This sets the flow control to hardware, software, or none. Default value: none.

- **all.dcd**
  - DCD signal (sets the tty parameter CLOCAL). Valid values are 0 or 1. If all.dcd=0, a connection request will be accepted regardless of the DCD signal and the connection will not be closed if the DCD signal is set to DOWN. If all.dcd=1 a connection request will be accepted only if the DCD signal is UP and the connection will be closed if the DCD signal is set to DOWN. Default value: 0.
**Serial Settings**

**all.sttyCmd (for CAS only)**

The TTY is programmed to work as configured and this user-specific configuration is applied over that serial port. Parameters must be separated by a space. The following example sets:

- `-igncr`
  
  This tells the terminal not to ignore the carriage-return on input,
  
- `-onlcr`
  
  Do not map newline character to a carriage return or newline character sequence on output,
  
- `opost`
  
  Post-process output,
  
- `-icrnl`
  
  Do not map carriage-return to a newline character on input.

```
all.sttyCmd -igncr -onlcr opost -icrnl
```

**DTR_reset (for CAS only)**

This parameter specifies the behavior of the DTR signal in the serial port configured with buffering or sniff session. If set to zero the DTR signal will be ON if there is a connection to the serial port, otherwise OFF. If set from 1 to 99 the DTR signal will be always ON. A value greater or equal 100 specifies for how long (in milliseconds) the DTR signal will be turned off before it is turned back on again when a connection to the serial port is closed. Example value: 3.

**Configuration for CAS**

**Browser Method**

**Step 1:** Point your browser to the Console Server.

In the address or location field of your browser type the Console Access Server's IP address. For example:

```
http://10.0.0.0
```

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

This will take you to the Configuration and Administration page.
Chapter 3 - Additional Features

Step 3: Select the Serial Ports link.
Click on the Serial Ports link on the Link Panel to the left of the page or in the Configuration section of the page. This will take you to the Port Selection page.

Step 4: Select port(s).
On the Port Selection page, choose all ports or an individual port to configure, from the dropdown menu. Click the Submit button. This will take you to the Serial Port Configuration page.

Step 5: Click the “CAS Profile” button.

Step 6: Scroll down to the Physical section.
You can change the settings for Speed, Data Size, Stop Bit, Parity, Flow Control, and DCD-sensitivity here.

Step 7: Click on the Submit button.

Step 8: Make the changes effective.
Click on the Administration > Run Configuration link, check the Serial Ports/Ethernet/Static Routes box and click on the Activate Configuration button.

Step 9: Click on the link Administration > Load/Save Configuration.

Step 10: Click the Save Configuration to Flash button.
The configuration was saved in flash.

Wizard Method

Step 1: Bring up the wizard.
At the command prompt, type the following to bring up the CAS Terminal Settings custom wizard:

```
wiz --sset cas
```

Screen 1 will appear.
Serial Settings

**Screen 1:**

***********************************************************
********* CONFIGURATION WIZARD ***********
***********************************************************

INSTRUCTIONS for using the Wizard:
You can:
1) Enter the appropriate information for your system and press ENTER. Enter '#' if you want to deactivate that parameter 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...

**Screen 2:**

***********************************************************
********* CONFIGURATION WIZARD ***********
***********************************************************

Current configuration:
(The ones with the '#' means it's not activated.)

all.speed : 9600
all.datasize : 8
all.stopbits : 1
all.parity : none
all.flow : none
all.dcd : 0
all.DTR_reset : 100
all.sttyCmd : #
Set to defaults? (y/n) [n] :

Screen 3:

***********************************************************
********* C O N F I G U R A T I O N  W I Z A R D ***********
***********************************************************
ALL.SPEED - The data speed in bits per second (bps) of all ports.
all.speed[9600] :

ALL.DATASIZE - The data size in bits per character of all ports.
all.datasize[8] :

Screen 4:

***********************************************************
********* C O N F I G U R A T I O N  W I Z A R D ***********
***********************************************************

ALL.STOPBITS - The number of stop bits for all ports.
all.stopbits[1] :

ALL.PARITY - The parity for all ports.
(e.g. none, odd, even)
all.parity[none] :
**Screen 5:**

***********************************************************
********* C O N F I G U R A T I O N W I Z A R D ***********
***********************************************************

ALL.FLOW - This sets the flow control to hardware, software, or none. (e.g. hard, soft, none)

all.flow[none] :

ALL.DCD - DCD signal (sets the tty parameter CLOCAL). Valid values are 0 or 1. In a socket session, if all.dcd=0, a connection request (telnet or ssh) will be accepted regardless of the DCD signal and the connection will not be closed if the DCD signal is set to DOWN. In a socket connection, if all.dcd=1 a connection request will be accepted only if the DCD signal is UP and the connection (telnet or ssh) will be closed if the DCD signal is set to DOWN.

all.dcd[0] :

**Screen 6:**

***********************************************************
********* C O N F I G U R A T I O N W I Z A R D ***********
***********************************************************

ALL.DTR_RESET - This parameter specifies the behavior of the DTR signal in the serial port. If set to 0 the DTR signal will be ON if there is a connection to the serial port, otherwise it will be OFF. If set from 1 to 99 the DTR signal will be always ON. A value greater or equal to 100 specifies for how long (in milliseconds) the DTR signal will be turned off before it is turned back on again when a connection to the serial port is closed.

all.DTR_reset[100] :
ALL.STTYCMD - Tty settings after a socket connection to that serial port is established. The tty is programmed to work as a CAS profile and this user specific configuration is applied over that serial port. Parameters must be separated by space. (e.g. all.sttyCmd -igncr -onlcr opost -icrnl) - igncr tells the terminal not to ignore the carriage-return on input, -onlcr means do not map newline character to a carriage return/newline character sequence on output, opost represents post-process output, -icrnl means do not map carriage-return to a newline character on input.

all.sttyCmd[#] :

**Screen 7:**

***********************************************************
********* C O N F I G U R A T I O N W I Z A R D **********
***********************************************************
Current configuration:
(The ones with the '#' means it's not activated.)

all.speed : 9600
all.datasize : 8
all.stopbits : 1
all.parity : none
all.flow : none
all.dcd : 0
all.DTR_reset : 100
all.sttyCmd : #

Are these configuration(s) all correct? (y/n) [n] :

If you type 'n'
Type 'c' to go back and CORRECT these parameters or 'q' to QUIT :

Typing 'c' repeats the application, typing 'q' exits the entire wiz application

If you type 'y'
Discard previous port-specific parameters? (y/n) [n] :
**Serial Settings**

**Note:** Answering yes to this question will discard only the parameter(s) which you are currently configuring if they were configured for a specific port in a previous session. For instance, if you are currently configuring parameter, all.x, and there was a specific port, s2.x, configured; then, answering yes to this question will discard s2.x.

Type 'c' to CONTINUE to set these parameters for specific ports or 'q' to QUIT:

*Typing 'c' leads to Screen 8, typing 'q' leads to Screen 9.*

**Screen 8:**

******************************************************************************
********* CONFIGURATION WIZARD *********
******************************************************************************
You have 8 available ports on this system.

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

**Note:** The number of available ports depends on the system you are on. Typing in a valid port number repeats this program except this time it's configuring for the port number you have chosen. Typing 'q' leads to Screen 9.
Chapter 3 - Additional Features

Screen 9:

***********************************************************
********* C O N F I G U R A T I O N W I Z A R D ***********
***********************************************************

(Note: If you are NOT connected to this unit through a console, and you have just reconfigured the IP of this unit, activating the new configurations may cause you to lose connection. In that case, please reconnect to the unit by the new IP address, and manually issue a saveconf to save your configurations to flash.)

Do you want to activate your configurations now? (y/n) [n]:

Screen 10:

***********************************************************
********* C O N F I G U R A T I O N W I Z A R D ***********
***********************************************************

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.

If you choose to save to flash, your configurations thus far will still be in the memory of the system even after you reboot it. If you don't save to flash and if you were to reboot the system, all your new configurations will be lost and you will have to reconfigure the system.

Do you want to save your configurations to flash? (y/n) [n]:

User Guide 203
Serial Settings

CLI Method

To configure line parameters for a specific serial port.

**Step 1:** At the command prompt, type in the appropriate command to configure desired parameters.

To activate the serial port. \(<\text{string}>\) should be \(\text{ttyS}<\text{serial port number}>\):

```
config configure line <serial port number> tty <string>
```

To configure speed:

```
config configure line <serial port number> speed <number>
```

To configure datasize:

```
config configure line <serial port number> datasize <number>
```

To configure stopbits:

```
config configure line <serial port number> stopbits <number>
```

To configure parity:

```
config configure line <serial port number> parity <string>
```

To configure flow:

```
config configure line <serial port number> flow <string>
```

To configure dcd:

```
config configure line <serial port number> dcd <number>
```

To configure DTR_reset:

```
config configure line <serial port number> dtr_reset <number>
```

To configure sttyCmd:

```
config configure line <serial port number> sttycmd <string>
```
Chapter 3 - Additional Features

Step 2: Activate and Save.

To activate your new configurations and save them to flash, type:

```
config write
```

(This is essentially typing `signal_ras hup` and `saveconf` from the normal terminal prompt.)

Tip. You can configure all the parameters for a serial port in one line:

```
config configure line <serial port number> tty <string> speed <number> datasize <number> stopbits <number> parity <string> flow <string> dcd <number> dtr_reset <number> sttycmd <string>
```

Configuration for TS

Browser Method

See the browser method for the CAS, earlier in this section. The only difference for TS is that “TS Profile” button should be clicked in Step 5.

Wizard Method

Step 1: Bring up the wizard.

At the command prompt, type the following to bring up the TS Terminal Settings custom wizard:

```
wiz --sset ts
```
Serial Settings

---

**Note:** Screens 1-5 are the same as those of the previous wizard for sset cas, thus, they are omitted here. The only difference between this feature and the CAS wizard is the parameter sttyCmd and DTR_reset. In the TS configuration, neither of these parameters is requested.

---

**Screen 6:**

***********************************************************
********* C O N F I G U R A T I O N   W I Z A R D **********
***********************************************************

Current configuration:
(The ones with the '#' means it's not activated.)

all.speed : 9600
all.datasize : 8
all.stopbits : 1
all.parity : none
all.flow : none
all.dcd : 0

Are these configuration(s) all correct? (y/n) [n] :

If you type 'n':
Type 'c' to go back and CORRECT these parameters
or 'q' to QUIT:

Typing 'c' repeats the application, typing 'q' exits the entire wiz application.

If you type 'y':
Type 'c' to CONTINUE to set these parameters for specific ports or 'q' to QUIT:

Typing 'c' leads to Screen 7 typing 'q' leads to Screen 8.
Chapter 3 - Additional Features

**Screen 7:**

***********************************************************
********* C O N F I G U R A T I O N  W I Z A R D ***********
***********************************************************
You have 8 available ports on this system.

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

**Note:** The number of available ports depends on the system you are on. Typing in a valid port number repeats this program except this time it's configuring for the port number you have chosen. Typing 'q' leads to Screen 8.

**Screen 8:**

***********************************************************
********* C O N F I G U R A T I O N  W I Z A R D ***********
***********************************************************

(Note: If you are NOT connected to this unit through a console, and you have just reconfigured the IP of this unit, activating the new configurations may cause you to lose connection. In that case, please reconnect to the unit by the new IP address, and manually issue a saveconf to save your configurations to flash.)

Do you want to activate your configurations now? (y/n) [y] :
Screen 9:
***********************************************************
********* C O N F I G U R A T I O N   W I Z A R D **********
***********************************************************

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.

If you choose to save to flash, your configurations thus far will still be in the memory of the system even after you reboot it. If you don't save to flash and if you were to reboot the system, all your new configurations will be lost and you will have to reconfigure the system.

Do you want to save your configurations to flash? (y/n) [n] :

CLI Method
To configure line parameters for a specific serial port:

Step 1: At the command prompt, type in the appropriate command to configure desired parameters.
  To activate the serial port. <string> should be ttyS<serial port number>:

    config configure line <serial port number> tty <string>

  To configure speed:

    config configure line <serial port number> speed <number>

  To configure datasize:

    config configure line <serial port number> datasize <number>

  To configure stopbits:

    config configure line <serial port number> stopbits <number>
To configure parity:

```
configure line <serial port number> parity <string>
```

To configure flow:

```
config configure line <serial port number> flow <string>
```

To configure dcd:

```
config configure line <serial port number> dcd <number>
```

**Tip.** You can configure all the parameters for a serial port in one line:

```
config configure line <serial port number> tty <string> speed <number> datasize <number> stopbits <number> parity <string> flow <string> dcd <number>
```

**Step 2: Activate and Save.**

To activate your new configurations and save them to flash, type:

```
config write
```

(This is essentially typing `signal_ras hup` and `saveconf` from the normal terminal prompt.)

**Configuration for Dial-in Access**

**Browser Method**

See the browser method for the CAS, earlier in this section. The only difference for Dial-in is that the “Dial-in Profile” button should be clicked in Step 5.
Serial Settings

CLI Method

To configure line parameters for a specific serial port:

**Step 1:** At the command prompt, type in the appropriate command to configure desired parameters.

To activate the serial port. `<string>` should be `ttyS<serial port number>`:

```plaintext
config configure line <serial port number> tty <string>
```

To configure speed:

```plaintext
config configure line <serial port number> speed <number>
```

To configure datasync:

```plaintext
config configure line <serial port number> datasync <number>
```

To configure stopbits:

```plaintext
config configure line <serial port number> stopbits <number>
```
Chapter 3 - Additional Features

**Session Sniffing**

**Versions 1.3.2 and earlier**

The Cyclades-TS allows a maximum of two connections to each serial port, as follows:

- One common session: user can execute read and write commands to the tty port. Session can be established by a regular user or by an administrator.

- One sniffer session: user can execute only read commands, in order to monitor what is going on in the other (main) session. Session can only be established by an administrator, defined by the parameter all.admin_users or sN.admin_users in the file pslave.conf (exception: authentication none - anyone can open a sniffer).

The first connection always opens a common session. After the second connection has been established and the user is authenticated, the Cyclades-TS shows the following menu to the administrator user:

```
* *
* * * ttySN is being used by (<user_name>) !!! *
* *
1 - Assume the main session
2 - Initiate a sniff session
3 - Quit
Enter your option:
```

If the second user is not an administrator, his connection is automatically refused. This description is valid for all of the available protocols (socket_server, socket_ssh or raw_data).
Session Sniffing

Versions 1.3.3 and later

You can open more than one common and sniff session at the same port. For this purpose, the following configuration items are available in the file pslave.conf:

- all.multiple_sessions: If it is configured as no, only two users can connect to the same port simultaneously. If it is configured as yes, more than two simultaneous users can connect to the same serial port. A “Sniffer menu” will be presented to the user and they can choose either to open a sniff session; to open a read and/or write session; to cancel a connection; or to send a message to other users connected to the same serial port. If it is configured as “RW_sessions,” only read and/or write sessions will be opened, and the sniffer menu won’t be presented. If it is configured as “sniff_session” only, a sniff session will be opened, and the sniffer menu won’t be presented. Default value: no.

- sN.multiple_sessions: Valid only for port N. If it is not defined, it will assume the value of all.multiple_sessions.

- all.multiuser_notif - Multiple User notification selects if users of a certain serial port should receive a warning message every time a new user logs in or out. By default this parameter is not activated. The warning messages doesn’t go to the buffering file and will be like the following example:

  WARNING: New user connected to this port.
  Current number of users: x

  or

  WARNING: User disconnection from this port.
  Current number of users: x

  Where x is the current number of connected users. The last user will know he/she is alone again when x = 1.

- sN.multiuser_notif - Valid only for port N. If it is not defined, it will assume the value of all.multiuser_notif.

- all.escape_char: Valid for all the serial ports; this parameter will be used to present the menus below to the user. Only characters from ‘^a’ to ‘^z’ (i.e., CTRL-A to CTRL-Z) will be accepted. The default value is ‘^z’ (CTRL-Z).

- sN.escape_char: Valid only for port N; this parameter will be used to present the menus below to the user. Only characters from ‘^a’ to ‘^z’ (i.e. CTRL-A to CTRL-Z) will be accepted. If it is not defined, it will assume the value of all.escape_char.
Chapter 3 - Additional Features

When multiple sessions are allowed for one port, the behavior of the Cyclades-TS will be as follows:

1. The first user to connect to the port will open a common session.

2. From the second connection on, only admin users will be allowed to connect to that port. The Cyclades-TS will send the following menu to these administrators (defined by the parameter all.admin_users or sN.admin_users in the file pslave.conf):
* * * ttySN is being used by (<first_user_name>) !!!

1 - Initiate a regular session
2 - Initiate a sniff session
3 - Send messages to another user
4 - Kill session(s)
5 - Quit

Enter your option:

If the user selects 1 - *Initiate a regular session*, s/he will share that serial port with the users that were previously connected. S/he will read everything that is received by the serial port, and will also be able to write to it.

If the user selects 2 - *Initiate a sniff session*, s/he will start reading everything that is sent and/or received by the serial port, according to the parameter all.sniff_mode or sN.sniff_mode (that can be in, out or i/o).

When the user selects 3 - *Send messages to another user*, the Cyclades-TS will send the user’s messages to all the sessions, but not to the tty port. Everyone connected to that port will see all the “conversation” that’s going on, as if they were physically in front of the console in the same room. These messages will be formatted as:

[Message from user/PID] <<message text goes here>> by the TS

To inform the Cyclades-TS that the message is to be sent to the serial port or not, the user will have to use the menu.

If the administrator chooses the option 4 - *Kill session(s)*, the Cyclades-TS will show him/her a list of the pairs PID/user_name, and s/he will be able to select one session typing its PID, or
Chapter 3 - Additional Features

“all” to kill all the sessions. If the administrator kills all the regular sessions, his session initiates as a regular session automatically.

Option 5 - Quit will close the current session and the TCP connection.

Only for the administrator users:
Typing all.escape_char or sN.escape_char from the sniff session or “send message mode” will make the TS show the previous menu. The first regular sessions will not be allowed to return to the menu. If you kill all regular sessions using the option 4, your session initiates as a regular session automatically.

Parameters Involved and Passed Values
Sniffing involves the following parameters:

- **all.admin_users**
  - This parameter determines which users can receive the sniff menu. When users want access per port to be controlled by administrators, this parameter is obligatory and authtype must not be none. User groups (defined with the parameter conf.group) can be used in combination with user names in the parameter list. Example values: peter, john, user_group.

- **all.sniff_mode**
  - This parameter determines what other users connected to the very same port (see parameter admin_users below) can see of the session of the first connected user (main session): in shows data written to the port, out shows data received from the port, and i/o shows both streams, whereas no means sniffing is not permitted. The second and later sessions are called sniff sessions and this feature is activated whenever the protocol parameter is set to socket_ssh or socket_server. Example value: out.

- **all.escape_char**
  - This parameter determines which character must be typed to make the session enter menu mode. The possible values are <CTRL-a> to <CTRL-z>. Represent the CTRL with carat: ^. This parameter is only valid when the port protocol is socket_server or socket_ssh. Default value is ^z.
Session Sniffing

all.multiple_sessions If it is configured as *no*, only two users can connect to the same port simultaneously. If it is configured as *yes*, more than two simultaneous users can connect to the same serial port. A “Sniffer menu” will be presented to the user and they can choose either to open a sniff session; to open a read and/or write session; to cancel a connection; or to send a message to other users connected to the same serial port. If it is configured as “RW_sessions,” only read and/or write sessions will be opened, and the sniffer menu won’t be presented. If it is configured as “sniff_session” only, a sniff session will be opened, and the sniffer menu won’t be presented. Default value: no.

all.multiuser_notif Multiple User notification selects if users of a certain serial port should receive a warning message every time a new user logs in or out. By default this parameter is not activated. The warning messages doesn’t go to the buffering file and will be like the following example:

WARNING: New user connected to this port.
Current number of users: x

or

WARNING: User disconnection from this port.
Current number of users: x

Where x is the current number of connected users. The last user will know he/she is alone again when x = 1.

Configuration for CAS

vi Method
Only the file /etc/portslave/pslave.conf has to be changed.

Browser Method
To configure Session Sniffing with your browser:

Step 1: Point your browser to the Console Server.
Chapter 3 - Additional Features

In the address or location field of your browser type the Console Access Server's IP address. For example:

http://10.0.0.0

Step 2: Log in as root and type the Web root password configured by the Web server.
This will take you to the Configuration and Administration page.

Step 3: Select the Serial Ports link.
Click on the Serial Ports link on the Link Panel to the left of the page or in the Configuration section of the page. This will take you to the Port Selection page.

Step 4: Select port(s).
On the Port Selection page, choose all ports or an individual port to configure, from the dropdown menu. Click the Submit button. This will take you to the Serial Port Configuration page.
Step 5: **Scroll down to the Sniff Session section.**

You can configure the appropriate values here.

<table>
<thead>
<tr>
<th>Sniff Session</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Sniff Session Mode</td>
<td>Not Sniff</td>
</tr>
<tr>
<td>Administrative Users</td>
<td></td>
</tr>
<tr>
<td>Escape Char from Sniff Mode</td>
<td></td>
</tr>
<tr>
<td>Allows Multiple Sniff Sessions</td>
<td>no</td>
</tr>
<tr>
<td>Multiple Sniff Session Notification</td>
<td>yes</td>
</tr>
</tbody>
</table>

*Figure 30: Sniff Session section of the Serial Port Configuration page*

Step 6: **Click on the Submit button.**

Step 7: **Make the changes effective.**

Click on the Administration > Run Configuration link, check the Serial Ports/Ethernet/Static Routes box and click on the Activate Configuration button.

Step 8: **Click on the link Administration > Load/Save Configuration.**

Step 9: **Click the Save Configuration to Flash button.**

The configuration was saved in flash.

**Wizard Method**

Step 1: **Bring up the wizard.**

At the command prompt, type the following to bring up the Sniffing custom wizard:

```
wiz --snf
```
Chapter 3 - Additional Features

Screen 1:

***********************************************************
********** C O N F I G U R A T I O N W I Z A R D **********
***********************************************************

INSTRUCTIONS for using the Wizard:
You can:
1) Enter the appropriate information for your system
   and press ENTER. Enter '#' if you want to
deactivate that parameter 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...

Screen 2:

***********************************************************
********** C O N F I G U R A T I O N W I Z A R D **********
***********************************************************

Current configuration:
(The ones with the '#' means it's not activated.)

all.admin_users : #
all.sniff_mode : out
all.escape_char : ^z
all.multiple_sessions : no
Session Sniffing

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

Screen 3:

******************************************************************************
************ CONFIGURATION WIZARD ************
******************************************************************************

ALL.ADMIN_USERS - This parameter determines which users can open a sniff session, which is where other users connected to the very same port can see everything that the first user is doing. The other users connected to the very same port can also cancel the first user's session (and take over). If the parameter, all.multiple_sessions, is configured as 'no', then only two users can connect to the same port simultaneously. If it is configured as 'yes', more simultaneous users can sniff the session or have read/write permissions.
(Please see details in Session Sniffing in Chapter 3 of the system's manual.)

all.admin_users[#] :

ALL.SNIFF_MODE - This parameter determines what other users connected to the very same port can see of the session of the first connected user (main session). The second session is called a sniff session and this feature is activated whenever the protocol is set to socket_ssh or socket_server.
(e.g. in -shows data written to the port, out -shows data received from the port, i/o -shows both streams.)

all.sniff_mode[out] :
Chapter 3 - Additional Features

Screen 4:

******************************************************************************
********* CONFIGURATION WIZARD *********
******************************************************************************

ALL.ESCAPE_CHAR - This parameter determines which character must be typed to make the session enter into "menu mode." The possible values are <CRTL-a> to <CRTL-z>, and this is only valid when the port protocol is socket_server or socket_ssh. Represent the CRTL character with '^'. Default value is ^z.

all.escape_char[^z] :

ALL.MULTIPLE_SESSIONS - Allows users to open multiple common and sniff sessions on the same port. The options are "yes," "no," "RW_session," or "sniff_session."
Default is set to "no."

all.multiple_sessions[no] :

Screen 5:

******************************************************************************
********* CONFIGURATION WIZARD *********
******************************************************************************

Current configuration:
(The ones with the '#' means it's not activated.)

all.admin_users : #
all.sniff_mode : out
all.escape_char : ^z
all.multiple_sessions : no
Are these configuration(s) all correct? (y/n) [n] :

If you type 'N'
Type 'c' to go back and CORRECT these parameters
or 'q' to QUIT :
Typing 'c' repeats the application, typing 'q' exits the entire wiz application

If you type 'Y'
Discard previous port-specific parameters? (y/n) [n] :

Note: Answering yes to this question will discard only the parameter(s) which you are currently configuring if they were configured for a specific port in a previous session. For instance, if you are currently configuring parameter, all.x, and there was a specific port, s2.x, configured; then, answering yes to this question will discard s2.x.

Type 'c' to CONTINUE to set these parameters for specific ports or 'q' to QUIT :

Typing 'c' leads to Screen 6, typing 'q' leads to Screen 7.

Screen 6:
******************************************************************************
********** CONFIGURATION WIZARD **********
******************************************************************************
You have 8 available ports on this system.

Type 'q' to quit, a valid port number[1-8], or anything else to refresh :
Chapter 3 - Additional Features

**NOTE:** The number of available ports depends on the system you are on. Typing in a valid port number repeats this program except this time it's configuring for the port number you have chosen. Typing 'q' leads to Screen 7.

**Screen 7:**

***********************************************************
********* C O N F I G U R A T I O N W I Z A R D ***********
***********************************************************

(Note: If you are NOT connected to this unit through a console, and you have just reconfigured the IP of this unit, activating the new configurations may cause you to lose connection. In that case, please reconnect to the unit by the new IP address, and manually issue a saveconf to save your configurations to flash.)

Do you want to activate your configurations now? (y/n) [y] :

**Screen 8:**

***********************************************************
********* C O N F I G U R A T I O N W I Z A R D ***********
***********************************************************

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.
If you choose to save to flash, your configurations thus far will still be in the memory of the system even after you reboot it. If you don’t save to flash and if you were to reboot the system, all your new configurations will be lost and you will have to reconfigure the system.

Do you want to save your configurations to flash? (y/n) [n] :

**CLI Method**

To configure certain parameters for a specific serial port:

**Step 1:** At the command prompt, type in the appropriate command to configure desired parameters.

To activate the serial port. `<string>` should be `ttyS<serial port number>` :

```
config configure line <serial port number> tty <string>
```

To configure admin_users:

```
config configure line <serial port number> adminusers <string>
```

To configure sniff_mode:

```
config configure line <serial port number> sniffmode <string>
```

To configure escape_char:

```
config configure line <serial port number> escape <string>
```

To configure multiple_sessions:

```
config configure line <serial port number> multiplesess <string>
```
Chapter 3 - Additional Features

Tip. You can configure all the parameters for a serial port in one line.

    config configure line <serial port number> tty <string>
    adminusers <string> sniffmode <string> escape <string>
    multiplesess <string>

Step 2: Activate and Save.

To activate your new configurations and save them to flash, type:

    config write
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.

The TS uses the net-snmp package (http://www.net-snmp.org).

**Important!** Check the SNMP configuration before gathering information about TS 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 TS cannot permit the public community to read SNMP information.

The net-snmp supports snmp version 1, 2 and 3. To use SNMP version 1 or 2 (community), you need to configure the communities in the snmp config file (/etc/snmp/snmpd.conf). To use SNMP version 3 (username/password), perform the following steps:

**Step 1:** Create a file `/etc/snmp/snmpd.local.conf` with the following line:

```
createUser <username> MD5 <password> DES
```

For example:

```
createUser usersnmp MD5 user_snmp_passwd DES
```

**Important!** The SNMP v3 password MUST have at least 8 characters. If a password with less than 8 characters is inserted, there will be no error messages, but the SNMP user will not be created.

**Step 2:** Edit the `/etc/snmp/snmpd.conf` file.

If the user has permission to read only, to add the line:

```
rouser <username> (ex.: rouser usersnmp).
```
Chapter 3 - Additional Features

If the user has permission to read and write, to add the line:

```
rwuser <username>  (ex.: rwuser usernmp).
```

**Step 3: Include the following line in /etc/config_files:**

```
/etc/snmp/snmpd.local.conf
```

You can configure the `/etc/snmp/snmpd.conf` file as indicated later in this section.

1. Snmp version 1
   - RFC1155 - SMI for the official MIB tree
   - RFC1213 - MIB-II

2. Snmp version 2
   - RFC2578 - Structure of Management Information Version 2 (SMIv2)
   - RFC2579 - Textual Conventions for SMIv2
   - RFC2580 - Conformance Statements for SMIv2

3. Snmp version 3
   - RFC2570 - Introduction to Version 3 of the Internet-standard Network Management Framework
   - RFC2571 - An Architecture for Describing SNMP Management Frameworks
   - RFC2572 - Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)
   - RFC2573 - SNMP Applications
   - RFC2574 - User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)
   - RFC2575 - View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)
   - RFC2576 - Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework
4. Private UCD SNMP mib extensions (enterprises.2021)
   - Information about memory utilization (/proc/meminfo)
   - Information about system status (vmstat)
   - Information about net-snmp packet

5. Private Cyclades Vendor MIB (enterprises.2925)
   - Cyclades-TSxx Remote Management Object Tree (cyclades.4). This MIB permits
     you to get informations about the product, to read/write some configuration items
     and to do some administration commands. (For more details see the cyclades.mib
     file.)

vi Method
Files to be changed:

/etc/snmp/snmpd.conf
This file has information about configuring for SNMP.

Step 1: Map the community name public into a security name.

    #       sec.name  source          community
    com2sec notConfigUser  default       public

Step 2: Map the security name into a group name.

    #       groupName      securityModel securityName
    group   notConfigGroup v1          notConfigUser
    #group   notConfigGroup v2c         notConfigUser

Step 3: Create a view to which the group has rights.

    #       name           incl/excl     subtree         mask(optional)
    view    all     included      .1

Step 4: Grant the group read-only access to the all view.
Chapter 3 - Additional Features

#       group          context sec.model sec.level prefix read   write
notif
access  notConfigGroup ""      any       noauth    exact all none none

Example:
# Here is a commented out example configuration that allows less
# restrictive access.

# YOU SHOULD CHANGE THE "COMMUNITY" TOKEN BELOW TO A NEW KEYWORD
# ONLY KNOWN AT YOUR SITE. YOU *MUST* CHANGE THE NETWORK TOKEN
# BELOW TO SOMETHING REFLECTING YOUR LOCAL NETWORK ADDRESS SPACE.

##       sec.name  source          community
#com2sec local     localhost       COMMUNITY
#com2sec mynetwork NETWORK/24      COMMUNITY

##     group.name sec.model  sec.name
#group MyRWGroup  any        local
#group MyROGroup  any        mynetwork
#
#group MyRWGroup  any        otherv3user
#...

##           incl/excl subtree                          mask
#view all    included  .1                               80
## -or just the mib2 tree-

```plaintext
#view mib2 included .iso.org.dod.internet.mgmt.mib-2 fc

##
context sec.model sec.level prefix read write notif
#access MyROGroup "" any noauth 0 all none none
#access MyRWGroup "" any noauth 0 all all all
```

---

SNMP

---

230

Cyclades-TS
Chapter 3 - Additional Features

Browser Method

To configure SNMP with your browser:

**Step 1:** **Point your browser to the Console Server.**
In the address or location field of your browser type the Console Access Server's IP address. For example:

http://10.0.0.0

**Step 2:** **Log in as root and type the Web root password configured by the Web server.**
This will take you to the Configuration and Administration page.

**Step 3:** **Click on the SNMP link.**
Select the SNMP link. The SNMP configuration file will appear in text mode.

**Step 4:** **Edit the configuration file and click on the Submit button**

**Step 5:** **Make changes effective.**
Click on the Administration > Run Configuration link. Check the SNMP box and click on the Activate Configuration button.

**Step 6:** **Click on the Administration > Load/Save Configuration and click on the Save to Flash button.**
This will save the file in the flash.
The syslog-ng daemon provides a modern treatment to system messages. Its basic function is to read and log messages to the system console, log files, other machines (remote syslog servers) and/or users as specified by its configuration file. In addition, syslog-ng is able to filter messages based on their content and to perform an action (e.g. to send an e-mail or pager message). In order to access these functions, the syslog-ng.conf file needs some specific configuration.

The configuration file (default: syslog-ng.conf) is read at startup and is reread after reception of a hangup (HUP) signal. When reloading the configuration file, all destination files are closed and reopened as appropriate. The syslog-ng reads from sources (files, TCP/UDP connections, syslogd clients), filters the messages and takes an action (writes in files, sends snmptrap, pager, e-mail or syslogs to remote servers).

There are five tasks required for configuring syslog-ng:

- Task 1: Define Global Options.
- Task 2: Define Sources.
- Task 3: Define Filters.
- Task 4: Define Actions (Destinations).
- Task 5: Connect all of the above.

The five tasks are explained in the following section “Syslog-ng and its Configuration” on page 239.
Port Slave Parameters Involved with syslog-ng

**conffacility**
This value (0-7) is the Local facility sent to the syslog-ng from PortSlave.

**conf.DB_facility**
This value (0-7) is the Local facility sent to the syslog-ng with data when syslog_buffering and/or alarm is active. When nonzero, the contents of the data buffer are sent to the syslogng every time a quantity of data equal to this parameter is collected. The syslog level for data buffering is hard coded to level five (notice) and facility local[0+ conf.DB_facility]. The file /etc/syslog-ng/syslog-ng.conf should be set accordingly for the syslog-ng to take some action. Example value: 0.

**all.syslog_buffering**
When nonzero, the contents of the data buffer are sent to the syslog-ng every time a quantity of data equal to this parameter is collected. The syslog message is sent to syslog-ng with NOTICE level and LOCAL[0+conf.DB_facility] facility.

Configuration for CAS, TS, and Dial-in Access

**vi Method**
To change the PortSlave parameters: edit the /etc/portslave/pslave.conf file.
To change the syslog-ng configuration: edit the /etc/syslog-ng/syslog-ng.conf file.

**Browser Method**
To configure the PortSlave parameters, see the Data Buffering section. To configure syslog via your Web browser:

**Step 1: Point your browser to the Console Server.**
In the address or location field of your browser type the Console Access Server's IP address. For example:

http://10.0.0.0

**Step 2: Log in as root and type the Web root password configured by the Web server.**
This will take you to the Configuration and Administration page.
Step 3: Click Syslog on the Configuration section.

Select the Syslog link. The following page will appear, giving information for configuring syslog:

![Syslog page 1](image)

**Figure 31: Syslog page 1**

Step 4: Edit the configuration file and click on the Submit button

Step 5: Make changes effective.

Click on the Administration > Run Configuration link. Check the Syslog-ng box and click on the Activate Configuration button.

Step 6: Click on the Administration > Load/Save Configuration and click on the Save to Flash button.

This will save the file in the flash.

Wizard Method

Step 1: Bring up the wizard.

At the command prompt, type the following to bring up the PortSlave parameters involved with the Syslog custom wizard:

```
wiz --sl
```
Chapter 3 - Additional Features

Screen 1 will appear.

**Screen 1:**

***********************************************************
********* C O N F I G U R A T I O N   W I Z A R D ***********
***********************************************************

INSTRUCTIONS for using the Wizard:
You can:
1) Enter the appropriate information for your system and press ENTER. Enter '#' if you want to deactivate that parameter 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...

**Screen 2:**

***********************************************************
********* C O N F I G U R A T I O N   W I Z A R D ***********
***********************************************************

Current configuration:
(The ones with the '#' means it's not activated.)

conf.facility : 7
conf.DB_facility : 0

Set to defaults? (y/n) [n] :
CONF.FACILITY - This value (0-7) is the Local facility sent to the syslog. The file /etc/syslog-ng/syslog-ng.conf contains a mapping between the facility number and the action. (Please see the 'Syslog-ng Configuration to use with Syslog Buffering Feature' section under Generating Alarms in Chapter 3 the system's manual for the syslog-ng configuration file.)

conf.facility[7] :

CONF.DB_FACILITY - This value (0-7) is the Local facility sent to the syslog with the data when syslog_buffering is active. The file /etc/syslog-ng/syslog-ng.conf contains a mapping between the facility number and the action. (Please see the 'Syslog-ng Configuration to use with Syslog Buffering Feature' section under Generating Alarms in Chapter 3 the system's manual for the syslog-ng configuration file.)

conf.DB_facility[0] :

Note: all.syslog_buffering is configured under the wiz -- db.
Chapter 3 - Additional Features

Screen 4:

***********************************************************
********* C O N F I G U R A T I O N   W I Z A R D *********
***********************************************************

Current configuration:
(The ones with the '#' means it's not activated.)

conf.facility : 7
conf.DB_facility : 0

Are these configuration(s) all correct? (y/n) [n] :

If you type 'n'
Type 'c' to go back and CORRECT these parameters
or 'q' to QUIT :
Typing 'c' repeats the application, typing 'q' exits the entire wiz application

If you type 'y' it leads to Screen 5.

Screen 5:

***********************************************************
********* C O N F I G U R A T I O N   W I Z A R D *********
***********************************************************

(Note: If you are NOT connected to this unit through a console, and you have just reconfigured the IP of this unit, activating the new configurations may cause you to lose connection. In that case, please reconnect to the unit by the new IP address, and manually issue a saveconf to save your configurations to flash.)

Do you want to activate your configurations now? (y/n) [y] :
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.

If you choose to save to flash, your configurations thus far will still be in the memory of the system even after you reboot it. If you don't save to flash and if you were to reboot the system, all your new configurations will be lost and you will have to reconfigure the system.

Do you want to save your configurations to flash? (y/n) [n] :

**CLI Method**

To configure certain parameters for a specific serial port:

**Step 1:** At the command prompt, type in the appropriate command to configure desired parameters.

To activate the serial port. <string> should be ttyS<serial port number>:

```bash
config configure line <serial port number> tty <string>
```

To configure conf.facility:

```bash
config configure conf facility <number>
```

To configure DB_facility:

```bash
config configure conf dbfacility <number>
```
Step 2: Activate and Save.

To activate your new configurations and save them to flash, type:

```
config write
```

(This is essentially typing `signal_ras bup` and `saveconf` from the normal terminal prompt.)

The Syslog Functions

This section shows the characteristics of the syslog-ng that is implemented for all members of the Cyclades-TS family. It is divided into three parts:

1. **Syslog-ng and its Configuration**
2. **Syslog-ng Configuration to use with Syslog Buffering Feature**
3. **Syslog-ng Configuration to use with Multiple Remote Syslog Servers**

Syslog-ng and its Configuration

The five tasks previously mentioned are detailed below.

**Task 1: Specify Global Options.**

You can specify several global options to syslog-ng in the options statement:

```
options { opt1(params); opt2(params); ... }
```

where `optn` can be any of the following:
**Syslog**

- **time_reopen(n)**: The time to wait before a dead connection is reestablished.
- **time_reap(n)**: The time to wait before an idle destination file is closed.
- **sync_freq(n)**: The number of lines buffered before written to file. (The file is synced when this number of messages has been written to it.)
- **mark_freq(n)**: The number of seconds between two MARKS lines.
- **log_fifo_size(n)**: The number of lines fitting to the output queue.
- **chain_hostname**: Enable/disable the chained hostname format.
  - (yes/no)
  - long_hostname: (yes/no)
- **use_time_recvd**: Use the time a message is received instead of the one specified in the message.
  - (yes/no)
- **use_dns**: Enable or disable DNS usage. syslog-ng blocks on DNS queries, so enabling DNS may lead to a Denial of Service attack.
  - (yes/no)
- **gc_idle_threshold(n)**: Sets the threshold value for the garbage collector, when syslog-ng is idle. GC phase starts when the number of allocated objects reach this number. Default: 100.
- **gc_busy_threshold(n)**: Sets the threshold value for the garbage collector. When syslog-ng is busy, GC phase starts.
- **create_dirs**: Enable the creation of new directories.
  - (yes/no)
- **owner(name)**: Set the owner of the created file to the one specified. Default: root.
- **group(name)**: Set the group of the created file to the one specified. Default: root.
- **perm(mask)**: Set the permission mask of the created file to the one specified. Default: 0600.
Chapter 3 - Additional Features

Task 2: Define sources.
To define sources use this statement:

```
source <identifier> { source-driver([params]); source
driver([params]); ...};
```

where:

- **identifier**: Has to uniquely identify this given source.
- **source-driver**: Is a method of getting a given message.
- **params**: Each source-driver may take parameters. Some of them are required, some of them are optional.

The following source-drivers are available:

- **a) internal()**: Messages are generated internally in syslog-ng.
- **b) unix-stream (filename [options])**: They open the given AF_UNIX socket, and start listening for messages.
  Options: owner(name), group(name), perm(mask) are equal global options
  and
- **unix-dgram (filename [options])**: `keep-alive(yes/no)` - Selects whether to keep connections opened when syslog-ng is restarted. Can be used only with unix_stream. Default: yes
  `max-connections(n)` - Limits the number of simultaneously opened connections. Can be used only with unix_stream. Default: 10.
c) tcp([options]) and udp([options])

These drivers let you receive messages from the network, and as the name of the drivers show, you can use both TCP and UDP.

None of tcp() and udp() drivers require positional parameters. By default they bind to 0.0.0.0:514, which means that syslog-ng will listen on all available interfaces.

Options:
- ip(<ip address>) - The IP address to bind to. Default: 0.0.0.0.
- port(<number>) - UDP/TCP port used to listen messages. Default: 514.
- max-connections(n) - Limits the number of simultaneously opened connections. Default: 10.

d) file(filename)

Opens the specified file and reads messages.

e) pipe(filename)

Opens a named pipe with the specified name, and listens for messages. (You'll need to create the pipe using mkfifo command).

Some Examples of Defining Sources

1) To read from a file:

source <identifier> {file(filename);};

Example to read messages from “/temp/file1” file:

source file1 {file(‘/temp/file1’);};

Example to receive messages from the kernel:

source s_kernel { file(‘/proc/kmsg’); };

2) To receive messages from local syslogd clients:

source sysl {unix-stream(‘/dev/log’);};

3) To receive messages from remote syslogd clients:

source s_udp { udp(ip(<cliente ip>) port(<udp port>)); };

Example to listen to messages from all machines on UDP port 514:

source s_udp { udp(ip(0.0.0.0) port(514));};
Chapter 3 - Additional Features

Example to listen to messages from one client (IP address=10.0.0.1) on UDP port 999:

```plaintext
source s_udp_10 { udp(ip(10.0.0.1) port(999)); }
```

**Task 3: Define filters.**

To define filters use this statement:

```plaintext
filter <identifier> { expression; }
```

where:

- **identifier**
  - Has to uniquely identify this given filter.

- **expression**
  - Boolean expression using internal functions, which has to evaluate to true for the message to pass.

The following internal functions are available:

- **a) facility(<facility code>)**
  - Selects messages based on their facility code.

- **b) level(<level code>) or priority(<level code>)**
  - Selects messages based on their priority.

- **c) program(<string>)**
  - Tries to match the <string> to the program name field of the log message.

- **d) host(<string>)**
  - Tries to match the <string> to the hostname field of the log message.

- **e) match(<string>)**
  - Tries to match the <string> to the message itself.

**Some Examples of Defining Filters**

1) To filter by facility:

```plaintext
filter f_facility { facility(<facility name>); }
```
Examples:

filter f_daemon { facility(daemon); };
filter f_kern { facility(kern); };
filter f_debug { not facility(auth, authpriv, news, mail); };

2) To filter by level:

filter f_level { level(<level name>); };

Examples:

filter f_messages { level(info .. warn) };
filter f_emergency { level(emerg) };
filter f_alert { level(alert) };

3) To filter by matching one string in the received message:

filter f_match { match('string'); };
Example to filter by matching the string “named”:

filter f_named { match('named') };

4) To filter ALARM messages (note that the following three examples should be one line):

filter f_alarm { facility(local[0+<conf.DB_facility>]) and level(info) and match('ALARM') and match('<your string>'); };

Example to filter ALARM message with the string “kernel panic”:

filter f_kpanic { facility(local[0+<conf.DB_facility>]) and level(info) and match('ALARM') and match('kernel panic'); };

Example to filter ALARM message with the string “root login”:

filter f_root { facility(local[0+<conf.DB_facility>]) and level(info) and match('ALARM') and match('root login'); };}
Chapter 3 - Additional Features

5) To eliminate sshd debug messages:

filter f_sshd_debug { not program('sshd') or not level(debug); };

6) To filter the syslog_buffering:

filter f_syslog_buf { facility(local[0+<conf.DB_facility>]) and level(notice); };

Task 4: Define Actions.
To define actions use this statement (note that the statement should be one line):

destination <identifier> { destination-driver([params]);
destination-driver([param]); ..};

where:

identifier Has to uniquely identify this given destination.

destination driver Is a method of outputting a given message.

params Each destination-driver may take parameters. Some of them required, some of them are optional.

The following destination drivers are available:

a) file(filename [options])
This is one of the most important destination drivers in syslog-ng. It allows you to output log messages to the named file. The destination filename may include macros (by prefixing the macro name with a '$' sign) which gets expanded when the message is written. Since the state of each created file must be tracked by syslog-ng, it consumes some memory for each file. If no new messages are written to a file within 60 seconds (controlled by the time_reap global option), it's closed, and its state is freed.
Available macros in filename expansion:
HOST - The name of the source host where the message originated from.
FACILITY - The name of the facility the message is tagged as coming from.
PRIORITY or LEVEL - The priority of the message.
PROGRAM - The name of the program the message was sent by.
YEAR, MONTH, DAY, HOUR, MIN, SEC - The year, month, day, hour, min, sec of the message was sent.
TAG - Equals FACILITY/LEVEL.
FULLHOST - The name of the source host and the source-driver:
<source-driver>@<hostname>
MSG or MESSAGE - The message received.
FULLDATE - The date of the message was sent.
Available options:
log_fifo_size(number) - The number of entries in the output file.
sync_freq(number) - The file is synced when this number of messages has been written to it.
owner(name), group(name), perm(mask) - Equals global options.
template("string") - Syslog-ng writes the "string" in the file. You can use the MACROS in the string.
encrypt(yes/no) - Encrypts the resulting file.
compress(yes/no) - Compresses the resulting file using zlib.

b) pipe(filename [options])
This driver sends messages to a named pipe. Available options:
owner(name), group(name), perm(mask) - Equals global options.
template("string") - Syslog-ng writes the "string" in the file. You can use the MACROS in the string.

c) unix-stream(filename) and unix-dgram(filename)
This driver sends messages to a UNIX socket in either SOCKET_STREAM or SOCK_DGRAM mode.

d) udp("<ip address>" port(number);) and tcp("<ip address>" port(number);)
This driver sends messages to another host (ip address/port) using either UDP or TCP protocol.

e) usertty(<username>)
This driver writes messages to the terminal of a logged-in username.
Some Examples of Defining Actions

1) To send e-mail:

```
destination <ident> { pipe('/dev/cyc_alarm' template('sendmail <pars>'))};
```

where ident: uniquely identifies this destination. Parameters:

- `-t <name>[,<name>]` To address
- `-c <name>[,<name>]` CC address
- `-b <name>[,<name>]` Bcc address
- `-r <name>[,<name>]` Reply-to address
- `-f <name>` From address
- `-s "<text>"` Subject
- `-m "<text message>"` Message
- `-h <IP address or name>` SMTP server
- `[p <port>]` Port used. default:25

To mount the message, use this macro:

- `$FULLDATE` The complete date when the message was sent.
- `$FACILITY` The facility of the message.
- `$PRIORITY` or `$LEVEL` The priority of the message.
- `$PROGRAM` The message was sent by this program (BUFFERING or SOCK).
Syslog
$HOST

The name of the source host.

$FULLHOST

The name of the source host and the source driver. Format:
<source>@<hostname>

$MSG or $MESSAGE

The message received.

Example to send e-mail to z@none.com (SMTP's IP address 10.0.0.2) from the e-mail address
a@none.com with subject “TS-ALARM”. The message will carry the current date, the hostname of this TS and the message that was received from the source.
destination d_mail1 {
pipe('/dev/cyc_alarm'
template('sendmail -t z@none.com -f a@none.com -s \'TS-ALARM\' \
-m \'$FULLDATE $HOST $MSG\' -h 10.0.0.2'));
};

2) To send to pager server (sms server):
destination <ident> {pipe(‘/dev/cyc_alarm’ template(‘sendsms
<pars>’));};
where ident: uniquely identify this destination
pars: -d <mobile phone number>
-m \’<message - max.size 160 characters>\’
-u <username to login on sms server>
-p <port sms - default : 6701>
<server IP address or name>
Example to send a pager to phone number 123 (Pager server at 10.0.0.1) with message
carrying the current date, the hostname of this TS and the message that was received from
the source:
destination d_pager {

248

Cyclades-TS


Chapter 3 - Additional Features

pipe('/dev/cyc_alarm'

template('sendsms -d 123 -m \'$FULLDATE $HOST $MSG\' 10.0.0.1')));

3) To send snmptrap:

destination <ident> {pipe('/dev/cyc_alarm' template('snmptrap <pars>')); }

where ident : uniquely identify this destination
pars : -v 1
<snmprapd IP address>
public : community
"" : enterprise-oid
"" : agent/hostname
<trap number> : 2-Link Down, 3-Link Up, 4-Authentication Failure
0 : specific trap
"" : host-uptime
.1.3.6.1.2.1.2.2.1.2.1 :interfaces.iftable.ifentry.ifdescr.1
s : the type of the next field (it is a string)
""<message - max. size 250 characters>""

Example to send a Link Down trap to server at 10.0.0.1 with message carrying the current date, the hostname of this TS and the message that was received from the source:

destination d_trap {
pipe("/dev/cycAlarm"

template("snmptrap -v1 10.0.0.1 public "" "" 2 0 "" "" .1.3.6.1.2.1.2.2.1.2.1 s "$FULLDATE $HOST $MSG" "");
};
4) To write in file:

destination d_file { file(<filename>);};

Example send message to console:

destination d_console { file("/dev/ttyS0");};

Example to write a message in /var/log/messages file:

destination d_message { file("/var/log/messages");};

5) To write messages to the session of a logged-in user:

destination d_user { usertty("<username>");};

Example to send message to all sessions with root user logged:

destination d_userroot { usertty("root");};

6) To send a message to a remote syslogd server:

destination d_udp { udp("<remote IP address>" port(514));};

Example to send syslogs to syslogd located at 10.0.0.1:

destination d_udp1 { udp("10.0.0.1" port(514));};

**Task 5: Connect all of the above.**

To connect the sources, filters, and actions, use the following statement. (Actions would be any message coming from one of the listed sources. A match for each of the filters is sent to the listed destinations.)

```diff
log { source(S1); source(S2); ... 
filter(F1);filter(F2);... 
destination(D1); destination(D2);... 
};
```
Chapter 3 - Additional Features

where:

$Sx$ Identifier of the sources defined before.

$Fx$ Identifier of the filters defined before.

$Dx$ Identifier of the actions/destinations defined before.

Examples:
1) To send all messages received from local syslog clients to console:

log { source(sysl); destination(d_console);};

2) To send only messages with level alert and received from local syslog clients to all logged
root user:

log { source(sysl); filter(f_alert); destination(d_userroot); };

3) To write all messages with levels info, notice, or warning and received from syslog clients
(local and remote) to /var/log/messages file:

log { source(sysl); source(s_udp); filter(f_messages); destination(d_messages); };

4) To send e-mail if message received from local syslog client has the string “kernel panic”:

log { source(sysl); filter(f_kpanic); destination(d_mail1); };

5) To send e-mail and pager if message received from local syslog client has the string “root
login”:

log { source(sysl); filter(f_root); destination(d_mail1); destination(d_pager); };

6) To send messages with facility kernel and received from syslog clients (local and remote)
to remote syslogd:

log { source(sysl); source(s_udp); filter(f_kern); destination(d-udp1); };
Syslog-ng Configuration to use with Syslog Buffering Feature

This configuration example uses the syslog buffering feature, and sends messages to the remote syslogd (10.0.0.1).

Step 1: Configure pslave.conf parameters.
In the pslave.conf file the parameters of the syslog buffering feature are configured as:

conf.DB_facility 1

all.syslog_buffering 100

Step 2: Add lines to syslog-ng.conf.
Add the following lines by vi or browser to the file:

```
# local syslog clients
source src { unix-stream("/dev/log"); };

destination d_buffering { udp("10.0.0.1"); };

filter f_buffering { facility(local1) and level(notice); };

# send only syslog_buffering messages to remote server
log { source(src); filter(f_buffering); destination(d_buffering); };
```

Syslog-ng Configuration to use with Multiple Remote Syslog Servers

This configuration example is used with multiple remote syslog servers.

Step 1: Configure pslave.conf parameters.
In the pslave.conf file the facility parameter is configured as:

conf.facility 1

Step 2: Add lines to syslog-ng.conf.
The syslog-ng.conf file needs these lines:

```
# local syslog clients
source src { unix-stream("/dev/log"); };
```
Chapter 3 - Additional Features

# remote server 1 - IP address 10.0.0.1 port default
destination d_udp1 { udp("10.0.0.1"); };
# remote server 2 - IP address 10.0.0.2 port 1999
destination d_udp2 { udp("10.0.0.2" port(1999)); };
# filter messages from facility local1 and level info to warning
filter f_local1 { facility(local1) and level(info..warn); };
# filter messages from facility local 1 and level err to alert
filter f_critic { facility(local1) and level(err .. alert); };
# send info, notice and warning messages to remote server udp1
log { source(src); filter(f_local1); destination(d_udp1); };
# send error, critical and alert messages to remote server udp2
log { source(src); filter(f_critic); destination(d_udp2); };

TCP Keepalive

The objective of this feature is to allow the TS and to recognize when the socket client (ssh or telnet) goes down without closing the connection properly. Currently, if this happens in a serial port the system administrator must close the connection manually or nobody else can access that port anymore.

How it works

The TCP engine of TS or will send a tcp keepalive message (ACK) to the client. If the maximum retry number is reached without an answer from the client, the connection is closed.
TCP Keepalive

How to Configure it

The configuration is done in the file `/bin/init_proc_fs` using the linux proc filesystem.

# Enable routing
echo 1 > /proc/sys/net/ipv4/ip_forward

# Enable TCP keepalive timer
echo 60 > /proc/sys/net/ipv4/tcp_keepalive_time
echo  2 > /proc/sys/net/ipv4/tcp_keepalive_probes

# Memory subsystem tuning
echo 0 0 > /proc/sys/vm/pagetable_cache
echo 2 > /proc/sys/vm/page-cluster
echo 16 32 48 > /proc/sys/vm/freepages
Chapter 3 - Additional Features

Terminal Appearance

You can change the format of the login prompt and banner that is issued when a connection is made to the system. Prompt and banner appearance can be port-specific as well.

Parameters Involved and Passed Values

Terminal Appearance involves the following parameters:

- **all.prompt**  
  This text defines the format of the login prompt. Expansion characters can be used here. Example value: %h login:

- **all.issue**  
  This text determines the format of the login banner that is issued when a connection is made to the Cyclades-TS. \n represents a new line and \r represents a carriage return. Expansion characters can be used here.

  *Value for this Example:*

  \r
  Welcome to terminal server %h port S%p \n  \r

- **all.lf_suppress**  
  This activates line feed suppression. When configured as 0, line feed suppression will not be performed. When 1, extra line feed will be suppressed.

- **all.auto_answer_input**  
  This parameter is used in conjunction with the next parameter, auto_answer_output. If configured and if there is no session established to the port, this parameter will constantly be compared and matched up to the string of bytes coming in remotely from the server. If a match is found, the string configured in auto_answer_output is sent back to the server. To represent the ESC character as part of this string, use the control character, ^[.
**Terminal Appearance**

`all.auto_answer_output` This parameter is used in conjunction with the previous parameter, `auto_answer_input`. If configured, and if there is no session established to the port, this parameter is sent back to the server when there is a match between the incoming data and `auto_answer_input`. To represent the ESC character as part of this string, use the control character, `^`.

---

**Configuration for CAS, TS, and Dial-in Access**

**Browser Method**

**Step 1:** **Point your browser to the Console Server.**
In the address or location field of your browser type the Console Access Server’s IP address. For example:

http://10.0.0.0

**Step 2:** **Log in as root and type the Web root password configured by the Web server.**
This will take you to the Configuration and Administration page.

**Step 3:** **Select the Serial Ports link.**
Click on the Serial Ports link on the Link Panel to the left of the page or in the Configuration section of the page. This will take you to the Port Selection page.

**Step 4:** **Select port(s).**
On the Port Selection page, choose all ports or an individual port to configure, from the dropdown menu. Click the Submit button. This will take you to the Serial Port Configuration page.

**Step 5:** **Scroll down to the Terminal Server section.**
You can change the settings for Banner Field (issue) and Login Prompt field here.

**Step 6:** **Click on the Submit button.**

**Step 7:** **Make the changes effective.**
Click on the Administration > Run Configuration link, check the Serial Ports/Ethernet/Static Routes box and click on the Activate Configuration button.
Chapter 3 - Additional Features

Step 8: Click on the link Administration > Load/Save Configuration.

Step 9: Click the Save Configuration to Flash button.

The configuration was saved in flash.

Wizard Method

Step 1: Bring up the wizard.
At the command prompt, type the following to bring up the Terminal Appearance custom wizard:

```
wiz --tl
```

Screen 1 will appear.

Screen 1:

***********************************************************
********* C O N F I G U R A T I O N W I Z A R D ***********
***********************************************************

INSTRUCTIONS for using the Wizard:
You can:
1) Enter the appropriate information for your system and press ENTER. Enter '#' if you want to deactivate that parameter 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...

Screen 2:

***********************************************************
********* CONFIGURATION WIZARD *********
***********************************************************
Current configuration: 
(The ones with the '#' means it's not activated.)

all.issue : \r\n\r\n\r\nWelcome to terminal server %h port $p \n\n\r\n\r\n
all.prompt : %h login:
all lfSuppress : 0
all auto_answer_input : #
all auto_answer_output : #

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

Screen 3:

***********************************************************
********* CONFIGURATION WIZARD *********
***********************************************************
ALL.ISSUE - This text determines the format of the login banner that is issued when a connection is made to the system. \n represents a new line and \r represents a carriage return.

all.issue[\r\n\r\nWelcome to terminal server %h port $p \n\r\n] :

ALL.PROMPT - This text defines the format of the login prompt.

all.prompt[%h login:] :
**Chapter 3 - Additional Features**

*Screen 4:*

*********************************************************
********** CONFIGURATION WIZARD **********
*********************************************************

ALL.LF_SUPPRESS - This activates line feed suppression. When configured as 0, line feed suppression will not be performed. When 1, extra line feed will be suppressed.

all.lf_suppress[0] :

ALL.AUTO_ANSWER_INPUT - This parameter is used in conjunction with the next parameter, auto_answer_output. Please refer to the manual for more info.

If configured and if there is no session established to the port, this parameter will constantly be compared and matched up to the string of bytes coming in remotely from the server. If a match is found, the string configured in auto_answer_output is sent back to the server. To represent the ESC character as part of this string, use the control character, ^[.

all.auto_answer_input[#] :

*Screen 5:*

*********************************************************
********** CONFIGURATION WIZARD **********
*********************************************************

ALL.AUTO_ANSWER_OUTPUT - This parameter is used in conjunction with the previous parameter, auto_answer_input. Please refer to the manual for more info.

If configured, and if there is no session established to the port, this parameter is sent back to the server when there is a match between the incoming data and auto_answer_input. To represent the ESC character as part of this string, use the control character, ^[.
Terminal Appearance

all.auto_answer_output[#] :

Screen 6:
***********************************************************
********* C O N F I G U R A T I O N   W I Z A R D ***********
***********************************************************
Current configuration:
(The ones with the '#' means it's not activated.)

all.issue : \r\n\Welcome to terminal server %h port $p \n\ 
\r\n\ all.prompt : %h login:
all.lf_suppress : 0
all.auto_answer_input : #
all.auto_answer_output : #

Are these configuration(s) all correct? (y/n) [n] :

If you type 'N'
Type 'c' to go back and CORRECT these parameters
or 'q' to QUIT :
Typing 'c' repeats the application, typing 'q' exits the entire wiz application

If you type 'Y'

Discard previous port-specific parameters? (y/n) [n] :

Note: Answering yes to this question will discard only the parameter(s) which you are currently configuring if they were configured for a specific port in a previous session. For instance, if you are currently configuring parameter, all.x, and there was a specific port, s2.x, configured; then, answering yes to this question will discard s2.x.

Type 'c' to CONTINUE to set these parameters for specific ports or 'q' to QUIT :

Typing 'c' leads to Screen 7, typing 'q' leads to Screen 8.
You have 8 available ports on this system.
Type 'q' to quit, a valid port number[1-8], or anything else to refresh :

(Note: If you are NOT connected to this unit through a console, and you have just reconfigured the IP of this unit, activating the new configurations may cause you to lose connection. In that case, please reconnect to the unit by the new IP address, and manually issue a saveconf to save your configurations to flash.)

Do you want to activate your configurations now? (y/n) [y] :

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.

If you choose to save to flash, your configurations thus
far will still be in the memory of the system even after you reboot it. If you don't save to flash and if you were to reboot the system, all your new configurations will be lost and you will have to reconfigure the system.

Do you want to save your configurations to flash? (y/n) [n] :

**CLI Method**

To configure certain parameters for a specific serial port:

**Step 1:** *At the command prompt, type in the appropriate command to configure desired parameters.*

To activate the serial port. <string> should be ttyS<serial port number>:

```
config configure line <serial port number> tty <string>
```

To configure issue:

```
config configure line <serial port number> issue <string>
```

To configure prompt:

```
config configure line <serial port number> prompt <string>
```

To configure lf_suppress:

```
config configure line <serial port number> lf <number>
```

To configure auto_answer_input:

```
config configure line <serial port number> auto_input <string>
```

To configure auto_answer_output:

```
config configure line <serial port number> auto_output <string>
```
Step 2: **Activate and Save.**

To activate your new configurations and save them to flash, type:

```
config write
```

(This is essentially typing `signal_ras hup` and `saveconf` from the normal terminal prompt.)
The content of the file /etc/TIMEZONE can be in one of two formats. The first format is used when there is no daylight savings time in the local time zone:

\texttt{std \hspace{1em} offset}

The \texttt{std} string specifies the name of the time zone and must be three or more alphabetic characters. The offset string immediately follows \texttt{std} and specifies the time value to be added to the local time to get \textit{Coordinated Universal Time} (UTC). The offset is positive if the local time zone is west of the Prime Meridian and negative if it is east. The hour must be between 0 and 24, and the minutes and seconds must be between 0 and 59.

The second format is used when there is daylight savings time:

\texttt{std \hspace{1em} offset \hspace{1em} dst \hspace{1em} [offset],start[/time],end[/time]}

There are no spaces in the specification. The initial \texttt{std} and \texttt{offset} specify the Standard Time zone, as described above. The \texttt{dst} string and \texttt{offset} specify the name and offset for the corresponding daylight savings time zone. If the \texttt{offset} is omitted, it defaults to one hour ahead of Standard Time.

The start field specifies when daylight savings time goes into effect and the end field specifies when the change is made back to Standard Time. These fields may have the following formats:

- \texttt{Jn} This specifies the Julian day, with \(n\) being between 1 and 365. February 29 is never counted even in leap years.
- \texttt{n} This specifies the Julian day, with \(n\) being between 1 and 365. February 29 is counted in leap years.
- \texttt{Mm.w.d} This specifies day, \(d\) (0 < \(d\) < 6) of week \(w\) (1 < \(w\) < 5) of month \(m\) (1 < \(m\) < 12). Week 1 is the first week in which day \(d\) occurs and week 5 is the last week in which day \(d\) occurs. Day 0 is a Sunday.

The time fields specify when, in the local time currently in effect, the change to the other time occurs. If omitted, the default is 02:00:00.
In the example below:

GST+7DST+6,M4.1.0/14:30,M10.5.6/10

Daylight Savings Time starts on the first Sunday of April at 2:30 p.m. and it ends on the last Saturday of October at 10:00 a.m.

**How to set Date and Time**

The date command prints or sets the system date and time. Format of the command:

date MMDDhhmmCCYY

where:

- MM = month
- DD = day
- hh = hour
- mm = minute
- CC = century
- YY = year

For example:

date 101014452002

produces:

Thu Oct 10 14:45:00 DST 2002

The DST is because it was specified in /etc/TIMEZONE.

**Automatically adjust for Daylight Savings Time:**

Here is an example of /etc/TIMEZONE which will adjust for Central Standard Time/Central Daylight Savings Time in the USA:

CST+6CDST+5,M4.1.0,M10.5.0

Explanations:
CST+6 : We add 6 hours to CST to get GST/GMT.
CDST+5 : We add 5 hours to CDST to get GST/GMT.
M4.1.0 : Month 4 (April). Week=1. Day=0 (Sunday). This is the date we switch to CDST.
M10.5.0: Month 10 (October). Week=5 (Last week). Day=0 (Sunday). This is the date we switch back to CST.

For EST/EDST: EST+5EDST+4, M4.1.0, M10.5.0
For MST/MDST: MST+7MDST+6, M4.1.0, M10.5.0
For PST/PDST: PST+8PDST+7, M4.1.0, M10.5.0

NOTE: Remember to add an entry for /etc/TIMEZONE to /etc/config_files, if necessary, and to run the command "saveconf" to save any changes to flash.
Chapter 3 - Additional Features

TS110-only Analog and Digital Ports

Digital Ports
The digital ports are dry contact inputs. They are controlled via /dev/gpio, which provides 8 bit status of the 8 digital ports. The LSB of the status byte is digital port 1. When pin+ and pin- from the digital port are open (no contact between them), the port’s bit on the status byte is 0. If pin+ and pin- are closed, the port’s bit on the status byte is 1.

Analog Ports
The analog ports are accessed via /dev/adc1 and /dev/adc2. Each device controls a 15-bit Analog-to-Digital converter, which returns the digital value of the voltage between pin+ and pin- on the analog port. The Analog-to-Digital converter reports full scales (0x7FFF), when pin+ and pin- are open (no contact between them). If pin+ and pin- are closed, the Analog-to-Digital converter reports zero (0x0000). When applying 10 K ohms over pin+ and pin-, the Analog-to-Digital converter reports half scale (around 0x4000).

Port Utility (/bin/pu)
Port Utility is the native application to access the digital and analog ports. Here are some commands:

a) For general help:

[TS110/]# pu -h

Usage:

pu -<r> [-d device] [-p digital_port] -l -o -h

Options:

- r read from device.
- d device defines device to use.
- l list digital port status.
- o output in decimal format.
b) Check digital ports. On this example, digital port 1, 2 and 3 are closed. The command returns the status byte for all digital ports.

[TSL10]# pu -r -d /dev/gpio
07

c) Check digital ports as previously, but now with -l option. This option lists all ports and their status. On this example, digital port 1, 2 and 3 are closed.

[TSL10]# pu -r -d /dev/gpio -l
Digital Port Status: 07
   port 1 - closed
   port 2 - closed
   port 3 - closed
   port 4 - open
   port 5 - open
   port 6 - open
   port 7 - open
   port 8 - open

d) It is also possible to check just one digital port at a time. For that, the port number must be passed along with the parameter -p. For verbal report, use option -l. On this example, digital port 3 is closed.

[TSL10]# pu -r -d /dev/gpio -p 3 -l
Digital Port Status:
   port 3 - closed
Chapter 3 - Additional Features

[TS110]# pu -r -d /dev/gpio -p 3
1

e) On the previous command, if port is open, the command return 0.

[TS110]# pu -r -d /dev/gpio -p 3
0

f) Analog Port 1 is open. Reading full scale.

[TS110]# pu -r -d /dev/adcl
7fff

Analog and Digital ports on the Web

The analog port values and the digital port status are also available via web browser on Information Section.

Sending Warning Messages

TS110 can respond to events or status change by sending warning messages to the console port or e-mail messages via sendmail. The /etc/io_cron.src file and its /etc/io_cron.sh shell file are cron files that can be included in the /etc/crontab_files, as described on the crond utility configuration section.

The /etc/io_counter file is automatically created by /etc/io_cron.sh when it runs by the first time. The /etc/io_counter file holds the countdown counters with the number of messages per event. These counters limit the number of warning messages issued per event. Whenever a counter reaches zero, no further message is generated for that event. Value -1 means no limit. To restart any counter, either change the counter value in the file or remove the file itself, which forces all counters to their default values when the file is created again.
The /etc/io_cron.sh file has the counter default values that will be used to create the /etc/io_counter file. The counter default values, which can be modified by the user, are as follows:

ADC1=2 #Number of times Analog Port 1 warning will be sent
ADC2=2 #Number of times Analog Port 2 warning will be sent
DIG1=2 #Number of times Digital Port 1 warning will be sent
DIG2=2 #Number of times Digital Port 2 warning will be sent
DIG3=2 #Number of times Digital Port 3 warning will be sent
DIG4=2 #Number of times Digital Port 4 warning will be sent
DIG5=2 #Number of times Digital Port 5 warning will be sent
DIG6=2 #Number of times Digital Port 6 warning will be sent
DIG7=2 #Number of times Digital Port 7 warning will be sent
DIG8=2 #Number of times Digital Port 8 warning will be sent

The same /etc/io_cron.sh file also has the trigger values for each event and status. These values, which can be customized by the user, are as follows:

H_ADC1=65535  # Analog Port 1 A/D Converter high limit
L_ADC1=0      # Analog Port 1 A/D Converter low limit
H_ADC2=65535  # Analog Port 2 A/D Converter high limit
L_ADC2=0      # Analog Port 2 A/D Converter low limit
D1=0          # Digital Port 1 status (1-closed, 0-open)
D2=0          # Digital Port 2 status (1-closed, 0-open)
D3=0          # Digital Port 3 status (1-closed, 0-open)
D4=0          # Digital Port 4 status (1-closed, 0-open)
D5=0          # Digital Port 5 status (1-closed, 0-open)
D6=0          # Digital Port 6 status (1-closed, 0-open)
Chapter 3 - Additional Features

D7=0          # Digital Port 7 status (1-closed, 0-open)
D8=0          # Digital Port 8 status (1-closed, 0-open)

Therefore, if at any time, digital port 5 changes status, becoming different to the initial one defined on D5, a warning message is sent out.

In order to save any change done on these files, do not forget to include the file names in /etc/config_files and run saveconf.
Linux-PAM (Pluggable Authentication Modules for Linux) is a suite of shared libraries that enable the local system administrator to choose how applications authenticate users. In other words, without (rewriting and) recompiling a PAM-aware application, it is possible to switch between the authentication mechanism(s) it uses. Indeed, one may entirely upgrade the local authentication system without touching the applications themselves.

It is the purpose of the Linux-PAM project to separate the development of privilege-granting software from the development of secure and appropriate authentication schemes. This is accomplished by providing a library of functions that an application may use to request that a user be authenticated. This PAM library is configured locally with a system file, /etc/pam.conf to authenticate a user request via the locally available authentication modules. The modules themselves will usually be located in the directory /lib/security and take the form of dynamically loadable object files.

The Linux-PAM authentication mechanism gives to the system administrator the freedom to stipulate which authentication scheme is to be used. S/he has the freedom to set the scheme for any/all PAM-aware applications on your Linux system. That is, s/he can authenticate from anything as generous as simple trust (pam_permit) to something as severe as a combination of a retinal scan, a voice print and a one-time password!

Linux-PAM deals with four separate types of (management) task. These are: authentication management, account management, session management, and password management. The association of the preferred management scheme with the behavior of an application is made with entries in the relevant Linux-PAM configuration file. The management functions are performed by modules specified in the configuration file.

Following is a figure that describes the overall organization of Linux-PAM:
Figure 32: Data flow diagram of Linux-PAM

The left of the figure represents the application: Application X. Such an application interfaces with the Linux-PAM library and knows none of the specifics of its configured authentication method. The Linux-PAM library (in the center) consults the contents of the PAM configuration file and loads the modules that are appropriate for Application X. These modules fall into one of four management groups (lower center) and are stacked in the order they appear in the configuration file. These modules, when called by Linux-PAM, perform the various authentication tasks for the application. Textual information, required from or offered to the user can be exchanged through the use of the application-supplied conversation function.
The Linux-PAM Configuration File

Linux-PAM is designed to provide the system administrator with a great deal of flexibility in configuring the privilege-granting applications of their system. The local configuration of those aspects of system security controlled by Linux-PAM is contained in a single system file /etc/pam.conf. In this section we discuss the correct syntax of and generic options respected by entries to these files.

Configuration File Syntax

The reader should note that the Linux-PAM-specific tokens in this file are case-insensitive. The module paths, however, are case-sensitive since they indicate a file’s name and reflect the case-dependence of typical Linux file systems. The case-sensitivity of the arguments to any given module is defined for each module in turn.

In addition to the lines described below, there are two special characters provided for the convenience of the system administrator:

# Comments are preceded by this character and extend to the next end-of-line.
\ This character extends the configuration lines.

A general configuration line of the /etc/pam.conf file has the following form:

Service-name module-type control-flag module-path arguments

The meaning of each of these tokens is explained below.

Service-name The name of the service associated with this entry. Frequently the service name is the conventional name of the given application. For example, ‘ftpd’, ‘rlogind’, ‘su’, etc. There is a special service-name, reserved for defining a default authentication mechanism. It has the name ‘OTHER’ and may be specified in either lower or upper case characters. Note, when there is a module specified for a named service, the ‘OTHER’ entries are ignored.

Module-type One of (currently) the four types of module. The four types are as follows:
Chapter 3 - Additional Features

**Auth**- This module type provides two aspects of authenticating the user. First, it establishes that the user is who they claim to be, by instructing the application to prompt the user for a password or other means of identification. Second, the module can grant group membership, independently of the */etc/groups*, or other privileges through its credential-granting properties.

**Account**- This module performs non-authentication-based account management. It is typically used to restrict or permit access to a service based on the time of day, currently available system resources (maximum number of users) or perhaps the location of the applicant user—'root' login only on the console.

**Session**- Primarily, this module is associated with doing things that need to be done for the user before or after they can be given service. Such things include the logging of information concerning the opening or closing of some data exchange with a user, mounting directories, etc.

**Password**- This last module type is required for updating the authentication token associated with the user. Typically, there is one module for each ‘challenge/response’ based authentication (auth) module-type.

**Control-flag** The control-flag is used to indicate how the PAM library will react to the success or failure of the module it is associated with. Since modules can be stacked (modules of the same type execute in series, one after another), the control-flags determine the relative importance of each module. The application is not made aware of the individual success or failure of modules listed in the ‘*/etc/pam.conf*’ file. Instead, it receives a summary of success or fail responses from the Linux-PAM library. The order of execution of these modules is that of the entries in the */etc/pam.conf* file: earlier entries are executed before later ones. The control-flag can be defined with one of two syntaxes. The simpler (and historical) syntax for the control-flag is a single keyword defined to indicate the severity of concern associated with the success or failure of a specific module. There are four such keywords: required, requisite, sufficient and optional.

The Linux-PAM library interprets these keywords in the following manner:
**Linux-PAM**

**Module Path**

Module Path is the path-name of the dynamically loadable object file—the pluggable module itself. If the first character of the module path is ‘/’, it is assumed to be a complete path. If this is not the case, the given module path is appended to the default module path: /lib/security.

Currently, the Cyclades-TS has the following modules available:

**Required**

This indicates that the success of the module is required for the module-type facility to succeed. Failure of this module will not be apparent to the user until all of the remaining modules (of the same module-type) have been executed.

**Requisite**

This is similar to *required*. However, in the case that such a module returns a failure, control is directly returned to the application. The return value is that associated with the first required or requisite module to fail. Note that this flag can be used to protect against the possibility of a user getting the opportunity to enter a password over an unsafe medium. It is conceivable that such behavior might inform an attacker of valid accounts on a system. This possibility should be weighed against the significant concerns of exposing a sensitive password in a hostile environment.

**Sufficient**

The success of this module is deemed ‘sufficient’ to satisfy the Linux-PAM library that this module-type has succeeded in its purpose. In the event that no previous required module has failed, no more ‘stacked’ modules of this type are invoked. (Note: in this case subsequent required modules are not invoked.) A failure of this module is not deemed as fatal to satisfying the application.

**Optional**

As its name suggests, this control-flag marks the module as not being critical to the success or failure of the user’s application for service. In general, Linux-PAM ignores such a module when determining if the module stack will succeed or fail. However, in the absence of any definite successes or failures of previous or subsequent stacked modules this module will determine the nature of the response to the application. One example of this latter case is when the other modules return something like PAM_IGNORE.
<table>
<thead>
<tr>
<th>Module</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>pam_access</td>
<td>Provides logdaemon style login access control.</td>
</tr>
<tr>
<td>pam_deny</td>
<td>Deny access to all users.</td>
</tr>
<tr>
<td>pam_env</td>
<td>This module allows the (un)setting of environment variables. The use of previously set environment variables as well as PAM_ITEMS such as PAM_RHOST is supported.</td>
</tr>
<tr>
<td>pam_filter</td>
<td>This module was written to offer a plug-in alternative to programs like ttysnoop (XXX - need a reference). Since a filter that performs this function has not been written, it is currently only a toy. The single filter provided with the module simply transposes upper and lower case letters in the input and output streams. (This can be very annoying and is not kind to termcap-based editors.)</td>
</tr>
<tr>
<td>pam_group</td>
<td>This module provides group settings based on the user's name and the terminal they are requesting a given service from. It takes note of the time of day.</td>
</tr>
<tr>
<td>pam_issue</td>
<td>This module presents the issue file (/etc/issue by default) when prompting for a username.</td>
</tr>
<tr>
<td>pam_lastlog</td>
<td>This session module maintains the /var/log/lastlog file. It adds an open entry when called via the pam_open_session() function and completes it when pam_close_session() is called. This module can also display a line of information about the last login of the user. If an application already performs these tasks, it is not necessary to use this module.</td>
</tr>
<tr>
<td>pam_limits</td>
<td>This module, through the Linux-PAM open-session hook, sets limits on the system resources that can be obtained in a user session. Its actions are dictated more explicitly through the configuration file discussed in /etc/security/pam_limits.conf.</td>
</tr>
<tr>
<td>pam_listfile</td>
<td>The listfile module provides a way to deny or allow services based on an arbitrary file.</td>
</tr>
<tr>
<td>pam_motd</td>
<td>This module outputs the motd file (/etc/motd by default) upon successful login.</td>
</tr>
<tr>
<td>pam_nologin</td>
<td>Provides standard Unix nologin authentication.</td>
</tr>
</tbody>
</table>
**pam_permit**  This module should be used with extreme caution. Its action is to always permit access. It does nothing else.

**pam_radius**  Provides Radius server authentication and accounting.

**pam_rootok**  This module is for use in situations where the superuser wishes to gain access to a service without having to enter a password.

**pam_securetty**  Provides standard UNIX securetty checking.

**pam_time**  Running a well-regulated system occasionally involves restricting access to certain services in a selective manner. This module offers some time control for access to services offered by a system. Its actions are determined with a configuration file. This module can be configured to deny access to (individual) users based on their name, the time of day, the day of week, the service they are applying for and their terminal from which they are making their request.

**pam_tacplus**  Provides TacacsPlus Server authentication, authorization (account management), and accounting (session management).

**pam_unix**  This is the standard UNIX authentication module. It uses standard calls from the system’s libraries to retrieve and set account information as well as authentication. Usually this is obtained from the etc/passwd and the /etc/shadow file as well when shadow is enabled.

**pam_warn**  This module is principally for logging information about a proposed authentication or application to update a password.
Chapter 3 - Additional Features

Arguments

The arguments are a list of tokens that are passed to the module when it is invoked. They are much like arguments to a typical Linux shell command. Generally, valid arguments are optional and are specific to any given module. Invalid arguments are ignored by a module, however, when encountering an invalid argument, the module is required to write an error to syslog(3).

The following are optional arguments which are likely to be understood by any module. Arguments (including these) are in general, optional.

### pam_ldap

Pam_ldap looks for the ldap client configuration file “ldap.conf” in /etc/. Here’s an example of the ldap.conf file (partial):

```plaintext
# file name: ldap.conf

# This is the configuration file for the LDAP nameservice

# switch library and the LDAP PAM module.

# Your LDAP server. Must be resolvable without using LDAP.
host 127.0.0.1

# The distinguished name of the search base.
base dc=padl,dc=com
```

### Arguments

The arguments are a list of tokens that are passed to the module when it is invoked. They are much like arguments to a typical Linux shell command. Generally, valid arguments are optional and are specific to any given module. Invalid arguments are ignored by a module, however, when encountering an invalid argument, the module is required to write an error to syslog(3).

The following are optional arguments which are likely to be understood by any module. Arguments (including these) are in general, optional.

- **debug**
  - Use the syslog(3) call to log debugging information to the system log files.

- **no_warn**
  - Instruct module to not give warning messages to the application.

- **use_first_pass**
  - The module should not prompt the user for a password. Instead, it should obtain the previously typed password (from the preceding auth module), and use that. If that doesn’t work, then the user will not be authenticated. (This option is intended for auth and password modules only).
**try_first_pass**

The module should attempt authentication with the previously typed password (from the preceding auth module). If that doesn’t work, then the user is prompted for a password. (This option is intended for auth modules only).

**use_mapped_pass**

This argument is not currently supported by any of the modules in the Linux-PAM distribution because of possible consequences associated with U.S. encryption exporting restrictions.

**expose_account**

In general, the leakage of some information about user accounts is not a secure policy for modules to adopt. Sometimes information such as user names or home directories, or preferred shell, can be used to attack a user’s account. In some circumstances, however, this sort of information is not deemed a threat: displaying a user’s full name when asking them for a password in a secured environment could also be called being ‘friendly’. The expose_account argument is a standard module argument to encourage a module to be less discrete about account information as deemed appropriate by the local administrator. Any line in (one of) the configuration file(s), that is not formatted correctly will generally tend (erring on the side of caution) to make the authentication process fail. A corresponding error is written to the system log files with a call to syslog(3).
Chapter 3 - Additional Features

LDAP Authentication

LDAP server for Linux

Step 1: The RPMs required for the LDAP servers are:

- db (Sleepycat Berkeley Database)
- openssl (OpenSSL)
- openldap (OpenLDAP)

It's possible also to load the source codes and compile them, but it is easier to load these RPMs from the RedHat CDs.

Step 2: Go to the directory /etc/openldap or /usr/local/etc/openldap.

NOTE: the example uses /usr/local path. Change all references of /usr/local if the path is different, and check if the directory/file really exists.

```bash
cd /usr/local/etc/openldap
```

Step 3: Create the certificates:

```bash
ln -s /usr/local/bin/openssl .
ln -s /usr/local/ssl/misc/CA.pl .
PATH=$PATH:.
CA.pl -newca <-- answer questions, you MUST fill in "commonName"
CA.pl -newreq <-- repeat
CA.pl -signreq
mv newreq.pem ldapkey.pem
chmod 0600 ldapkey.pem
mv newcert.pem ldapcert.pem
```
LDAP Authentication

Step 4: Edit slapd.conf. The basic configuration to make it work is:

```plaintext
include /usr/local/etc/openldap/schema/core.schema
include /usr/local/etc/openldap/schema/cosine.schema

pidfile /usr/local/var/slapd.pid
argsfile /usr/local/var/slapd.args

TLSCipherSuite HIGH:MEDIUM:+SSLv2
TLSCertificateFile /usr/local/etc/openldap/ldapcert.pem
TLSCertificateKeyFile /usr/local/etc/openldap/ldapkey.pem
TLSCACertificateFile /usr/local/etc/openldap/demoCA/cacert.pem

database bdb
suffix "dc=cyclades,dc=com,dc=br"
rootdn "cn=admin,dc=cyclades,dc=com,dc=br"
rootpw bitadmin

directory /usr/local/var/openldap-data
index objectClass eq
```

Step 5: Start LDAP server. This is done by the command:

```plaintext
/usr/local/libexec/slapd -h "ldap:/// ldaps:///"
```

This will allow the LDAP server accept both secured mode and non-secure mode.
Step 6: Add entries.

Example:

```
ldapadd -x -D "cn=admin,dc=cyclades,dc=com,dc=br" -w bitadmin
dn: uid=cyuser,dc=cyclades,dc=com,dc=br
objectClass: person
objectClass: uidobject
uid: cyuser
cn: Cyclades User
sn: Fujimoto
userPassword: bituser
```

To list the entries:

```
ldapsearch -x -D "cn=admin,dc=cyclades,dc=com,dc=br" -w bitadmin
'(objectClass=*)'
```

This is enough to set up a LDAP server with some users, for PAM authentication purposes. In order to configure the TS:

Step 1: Configure all.protocol as ldap, in /etc/portslave/pslave.conf

Step 2: Edit /etc/ldap.conf. Edit the following parameters:

```
host 200.246.93.95 <= LDAP server IP address or name
base dc=cyclades,dc=com,dc=br <= distinguished name of the search base
uri ldaps://200.246.93.95 <= to use secure LDAP
```
LDAP Authentication

For Active Directory

A Windows 2000 or Windows 2003 Server edition is necessary. In the Cyclades-TS side, the /etc/ldap.conf file must be configured.

What needs to be set in the /etc/ldap.conf

# The Windows 2003 server IP address
host 200.246.93.118

# The Distinguished name (In our active directory, the format was set to cyclades.local)
base dc=CycladesCorporation,dc=local

# Here you can insert any user you had created, or the administrator user. I set
# the administrator user. I could not make the AD accept anonymous users to bind.
binddn cn=Administrator,cn=Users,dc=CycladesCorporation,dc=local

# Password for that user
bindpw Teste123

# PAM login attribute
pam_login_attribute sAMAccountName

# Update Active Directory password, by creating Unicode password and updating unicodePwd attribute.
pam_password ad
Default Policy

If a system is to be considered secure, it had better have a reasonably secure ‘OTHER’ entry. The following is a “severe” setting (which is not a bad place to start!):

```
#  
# default; deny access  
#  
OTHER auth required pam_deny.so
OTHER account required pam_deny.so
OTHER password required pam_deny.so
OTHER session required pam_deny.so
```

While fundamentally a secure default, this is not very sympathetic to a misconfigured system. For example, such a system is vulnerable to locking everyone out should the rest of the file become badly written.

The module pam_deny not very sophisticated. For example, it logs no information when it is invoked, so unless the users of a system contact the administrator when failing to execute a service application, the administrator may not know for a long while that his system is misconfigured.

The addition of the following line before those in the above example would provide a suitable warning to the administrator.

```
#  
# default; This application is not configured  
#  
OTHER auth required pam_warn.so
OTHER password required pam_warn.so
```

Having two “OTHER auth” lines is an example of stacking.
LDAP Authentication

On a less sensitive computer, the following selection of lines (in /etc/pam.conf) is likely to mimic the historically familiar Linux setup:

```
# default; standard UNIX access

OTHER auth required pam_unix_auth.so
OTHER account required pam_unix_acct.so
OTHER password required pam_unix_passwd.so
OTHER session required pam_unix_session.so
```

In general this will provide a starting place for most applications.

In addition to the normal applications: login, su, sshd, passwd, and pppd. Cyclades also has made portslave a PAM-aware application. The portslave requires four services configured in pam.conf. They are local, remote, radius, and tacplus. The portslave PAM interface takes any parameter needed to perform the authentication in the serial ports from the file pslave.conf. The pslave.conf parameter all.authtype determines which service(s) should be used.

```
# WARNING. The services tacacs, s_tacacs, radius, s_radius, local, s_local,
# and remote are used by the Cyclades applications portslave,
# socket_server, socket_ssh, and raw_data and should not be changed
```
Chapter 3 - Additional Features

# by the administrators unless he knows what he is doing.
#
# The PAM configuration file for the `ldap' service
#
ldapauth sufficient pam_ldap.so
ldapaccount required pam_ldap.so
ldapsession required pam_ldap.so

#
# The PAM configuration file for the `ldapdownlocal' service
# If LDAP server is down, uses the local service
#
ldapdownlocal auth\
  [ success=done new_auth_tok_reqd=done authinfo_unavail=ignore default=die ] \ 
  pam_ldap.so
ldapdownlocal auth required pam_unix2.so
ldapdownlocal account \\n  [ success=done new_auth_tok_reqd=done authinfo_unavail=ignore default=die ] \ 
  pam_ldap.so
ldapdownlocal account required pam_unix2.so
ldapdownlocal session \\
  [ success=done new_auth_tok_reqd=done authinfo_unavail=ignore default=die ] \ 
  pam_ldap.so
ldapdownlocal session required pam_unix2.so

#
# The PAM configuration file for the `tacplus' service
#
tacplus auth requisite pam_securetty.so
tacplus auth required pam_tacplus.so encrypt
LDAP Authentication

tacplus auth   optional  pam_auth_srv.so

tacplus account required  pam_tacplus.so encrypt service=ppp protocol=lcp

tacplus session required  pam_tacplus.so encrypt service=ppp protocol=lcp

s_tacplus auth   requisite  pam_security.so

s_tacplus auth   required  pam_tacplus.so encrypt use_first_pass

s_tacplus account required  pam_tacplus.so encrypt service=ppp protocol=lcp

s_tacplus session required  pam_tacplus.so encrypt service=ppp protocol=lcp

#
# The PAM configuration file for the `radius' service
#

radius auth       requisite  pam_security.so

radius auth       required  pam_radius_auth.so

radius auth       optional  pam_auth_srv.so

radius account    required  pam_radius_auth.so

radius session    required  pam_radius_auth.so

s_radius auth       requisite  pam_security.so

s_radius auth       required  pam_radius_auth.so use_first_pass

s_radius account    required  pam_radius_auth.so

s_radius session    required  pam_radius_auth.so

#
# The PAM configuration file for the `local' service
#

local auth       requisite  pam_security.so

local auth       required  pam_unix2.so

local account    required  pam_unix2.so

local password   required  pam_unix2.so md5 use_authtok
Chapter 3 - Additional Features

local session required pam_unix2.so

s_local auth requisite pam_securetty.so
s_local auth required pam_unix2.so use_first_pass
s_local account required pam_unix2.so
s_local password required pam_unix2.so md5 use_authtok
s_local session required pam_unix2.so

#
# The PAM configuration file for the `remote' service
#
remoteauth required pam_permit.so
remoteaccount required pam_permit.so
remotepassword required pam_permit.so
remotesession required pam_permit.so

#
# The PAM configuration file for the `login' service
#
loginauth requisite pam_securetty.so
loginauth required pam_unix2.so
loginauth optional pam_group.so
loginaccount requisite pam_time.so
loginaccount required pam_unix2.so
loginpassword required pam_unix2.so md5 use_authtok
loginsession required pam_unix2.so
login session required pam_limits.so

#
# The PAM configuration file for the `xsh' service
LDAP Authentication

#
sshdauth  required  pam_unix2.so
sshdauth  optional  pam_group.so
sshdaaccount  requisite  pam_time.so
sshdaaccount  required  pam_unix2.so
sshdpassword  required  pam_unix2.so md5 use_authtok
sshdsession  required  pam_unix2.so
sshd  session  required  pam_limits.so

#
# The PAM configuration file for the `passwd' service
#
passwdpassword  required  pam_unix2.so md5
#
# The PAM configuration file for the `samba' service
#
sambaauth  required  pam_unix2.so
sambaaccount  required  pam_unix2.so

#
# The PAM configuration file for the `su' service
#
suauth  required  pam_wheel.so
suauth  sufficient  pam_rootok.so
suauth  required  pam_unix2.so
suaccount  required  pam_unix2.so
susession  required  pam_unix2.so

#
# Information for the PPPD process with the 'login' option.
#

Chapter 3 - Additional Features

ppp auth required pam_nologin.so
ppp auth required pam_unix2.so
ppp account required pam_unix2.so
ppp session required pam_unix2.so

# Information for the ipppd process with the 'login' option: local authent.
#
ippp auth required pam_nologin.so
ippp auth required pam_unix2.so
ippp account required pam_unix2.so
ippp session required pam_unix2.so

# Information for the ipppd process with the 'login' option: radius authent.
#ippauth required pam_radius_auth.so conf=/etc/raddb/server
#ippauth optional pam_auth_srv.so
#ippaccount required pam_radius_auth.so conf=/etc/raddb/server
#ippsession required pam_radius_auth.so conf=/etc/raddb/server

# The PAM configuration file for the `other' service
#
otherauth required pam_warn.so
otherauth required pamdeny.so
otheraccount required pamdeny.so
otherpassword required pam_warn.so
otherpassword required pamdeny.so
othersession required pamdeny.so
Reference

The Linux-PAM System Administrators’ Guide
Copyright (c) Andrew G. Morgan 1996-9. All rights reserved.
Email: morgan@linux.kernel.org
Chapter 3 - Additional Features

Power Management

The AlterPath PM is a family of intelligent power strips (IPDU - Integrated Power Distribution Units), which is used for power management. Through a serial port, the administrator can use the AlterPath PM to control all the equipment connected to its outlets, using operations like On, Off, Cycle, Lock, and Unlock.

Using the AlterPath PM and the Advanced Secure Console Port Server SSHAlterPath Console ServerCyclades-TS together, the administrator can have full control over his data center equipment. He can, for example, reboot the data center equipment when it crashes, without leaving his console session (telnet or ssh). To do that, he must simply press a configurable hotkey and select the appropriate option from the menu displayed in the session.

Configuration

This section covers only the software configuration for the Console Server when used in conjunction with the AlterPath PM. For hardware and cabling installation instructions for the AlterPath PM, Please refer to the AlterPath PM User Guide included in the product.

Figure 33: Configuration diagram
Figure 33: Configuration diagram shows a typical setup for the AlterPath PM and the Cyclades-TS. The AlterPath PM's serial console is connected to port YY of the Console Server, the server's serial console is connected to port YY of the Console Server, and the server's power plug is connected to power outlet ZZ on the AlterPath PM. These port denominations will be used in the descriptions below.

Port Slave Parameters Involved and Passed Values

There are two different types of parameters:

1. Parameters to the port XX where the AlterPath PM is connected:
   - sXX.protocol IPDU: New protocol Integrated Power Distribution Unit. For example: ipdu.
   - sXX.pmtype: The IPDU manufacturer. For example: cyclades.
   - sXX.pmusers: The user access list. For example: jane:1,2; john:3-8. The format of this field is:
     
     \[<username>:<outlet list>][;<username>:<outlet list>...]

     where <outlet list>'s format is:

     \[<outlet number>|<outlet start>-<outlet end>][,<outlet number>|<outlet start>-<outlet end>]...

     The list of users must be separated by semicolons (;); the outlets should be separated by commas (,) to indicate a list or with dashes (-) to indicate range; there should not be any spaces between the values.
   - sXX.pmNumOfOutlets: the number of outlets of the AlterPath PM. Default: 8.
   - sXX.pmsessions: Only users logged in with the connection method defined by this parameter will be allowed to access the IPDU unit.

2. Parameters to the other ports where the servers are connected:
   - all.protocol: Protocols for the CAS profile. For example: socket_server, socket_raw, socket_ssh.
   - all.pmkey: The hot-key that starts a power management session. Default: ^p (Ctrl-p).
Chapter 3 - Additional Features

- sYY.pmoutlet: The outlet list where the server YY is plugged. The outlet is passed as a pair /PM_serial_port.outlet_number/. If the server has a dual power supply, the outlets are separated by space char. For example, one power supply is plugged in the second outlet of the IPDU connected in serial port 1. The other is plugged in the third outlet of the IPDU connected in serial port 5. The value is 1.2 5.3”.

sXXpmusers notes: The ellipses in the field format for sXX.pmusers means that you can add as many users as you need. The [] indicates that the parameter is optional, again indicating that you can configure more than one user. The separator is the semicolon, and spacing between the parameter and the variable matters in that a blank between names does not work.

  e.g. jane:1,2; john:3,4  does not work
  jane:1,2;john:3,4   works.

The users described in this parameter (sXX.pmusers) are related to the users logged in a console session. These users will not be able to do power management from any other means, unless they are root users.

Syslog Messages Generated by the IPDU
The IPDU generates syslog messages as a result of specific actions or conditions are as follows:

Table 15: IPDU Syslog messages format

<table>
<thead>
<tr>
<th>Level</th>
<th>Tag</th>
<th>Text</th>
</tr>
</thead>
<tbody>
<tr>
<td>alert</td>
<td>[PMD]-Serial Port p</td>
<td>Outlet X has been turned OFF by user &lt;username&gt;</td>
</tr>
<tr>
<td>alert</td>
<td>[PMD]-Serial Port p</td>
<td>Outlet X has been turned ON by user &lt;username&gt;</td>
</tr>
<tr>
<td>alert</td>
<td>[PMD]-Serial Port p</td>
<td>OVER CURRENT on IPDU #X (current: &lt;current detectec&gt; threshold:&lt;threshold configured&gt;)</td>
</tr>
<tr>
<td>alert</td>
<td>[PMD]-Serial Port p</td>
<td>One or more IPDUs were removed from the chain. This chain has now X IPDUs and Y outlets</td>
</tr>
</tbody>
</table>
Chapter 3 - Additional Features

Table 15: IPDU Syslog messages format

<table>
<thead>
<tr>
<th>Level</th>
<th>Tag</th>
<th>Text</th>
</tr>
</thead>
<tbody>
<tr>
<td>info</td>
<td>[PMD]-Serial Port p</td>
<td>One or more IPDUs were added to the chain. This chain has now X IPDUs and Y outlets</td>
</tr>
<tr>
<td>notice</td>
<td>[PMD]-Serial Port p</td>
<td>PMD has started on this port. The chain has X IPDUs and W outlets.</td>
</tr>
<tr>
<td>warning</td>
<td>[PMD]-Serial Port p</td>
<td>Current is now back to normal on IPDU #X (current: &lt;current detected&gt; threshold:&lt;threshold configured&gt;)</td>
</tr>
</tbody>
</table>

To not generate PMD syslog messages, the file `/etc/pmd.sh` has to be edited. The parameter DPARM must be changed from "" to "-s". After this, the command “saveconf” and "daemon restart PMD" must be run.

You can use the information provided in the table above to create filters and generate alarms about events that happens in the Cyclades-TS itself.

How to change the IPDU Password

Step 1: Change password using `pm` or `pmCommand`.

Step 2: Save the configuration in the IPDU.

Step 3: Edit the appropriate `/etc/pm.*` config file.

Step 4: Restart pmd to re-read the config file.

vi Method

The parameters described above must be changed by directly editing the `/etc/portsave/plsave.conf` file.
Chapter 3 - Additional Features

Browser Method

To configure Power Management to control IPDUs through the Advanced Secure Console Port Server SSH Web interface:

Step 1: **Point your browser to the Console Server.**
In the address or location field of your browser type the Console Access Server's IP address. For example:

http://10.0.0.0

Step 2: **Log in as root and type the Web root password configured by the Web server.**
This will take you to the Configuration and Administration page.

Step 3: **Select the Serial Ports link.**
Click on the Serial Ports link on the Link Panel to the left of the page or in the Configuration section of the page. This will take you to the Port Selection page.

Step 4: **Select the serial port where the IPDU is connected.**
After selecting the port, click the Connect button.

Step 5: **Click the PM8 profile button in the Wizard Section.**
This will automatically set the protocol to IPDU, the IPDU type to cyclades, and the number of outlets to 8.

Step 6: **Scroll down to the IPDU Section.**
Change the number of outlets and the user permissions in this section, if necessary.

Step 7: **Click the Submit button.**
If there are more IPDUs to be configured, repeat steps 4 to 7.

Step 8: **Select the port whose server has the power supply plugged into one or more IPDU outlets.**
After selecting the port, click the Submit button.

Step 9: **Configure the port as a Console Access Server.**
Read the Access Method section in Chapter 3 for details.
Chapter 3 - Additional Features

Step 10: Scroll down to the Power Management Section

Set the hotkey to access the power management menu and the outlet(s) the server is plugged into.

Step 11: Click on the Submit button.

Step 12: If there are more servers to be configured, repeat steps 8 to 11.

Step 13: Make the changes effective.

Click on the Administration > Run Configuration link, check the Serial Ports/ Ethernet/Static Routes box and click on the Activate Configuration button.

Step 14: Click on the link Administration > Load/Save Configuration.

Step 15: Click the Save Configuration to Flash button.

The configuration was saved in flash.

Wizard Method

Step 1: Bring up the wizard.

At the command prompt, type the following to bring up the Power Management custom wizard:

wiz --pm

Screen 1 will appear.

Screen 1:

***********************************************************
********* C O N F I G U R A T I O N   W I Z A R D ***********
***********************************************************

INSTRUCTIONS for using the Wizard:
You can:
1) Enter the appropriate information for your system and press ENTER. Enter '#' if you want to deactivate that parameter or
2) Press ENTER if you are satisfied with the value
Chapter 3 - Additional Features

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...

Screen 2:
***********************************************************
********* C O N F I G U R A T I O N   W I Z A R D ***********
***********************************************************
Current configuration:
(The ones with the '#' means it's not activated.)

all.protocol : ipdu
all.pmtype : cyclades
all.pmusers : #
all.pmoutlet : #
all.pmkey : ^p
all.pmNumOfOutlets : 8

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

Screen 3:
***********************************************************
********* C O N F I G U R A T I O N   W I Z A R D ***********
***********************************************************

ALL.PROTOCOL - The possible protocols are telnet (socket_server), ssh1/ssh2 (socket_ssh), raw data (raw_data), or integrated power distributed unit (ipdu).

all.protocol[ipdu] :
Chapter 3 - Additional Features

ALL.PMTYPE - Name of the IPDU manufacturer.

all.pmttype[cyclades] :

Screen 4:
********************************************************************************************************************
******** Configuration Wizard ********
********************************************************************************************************************

ALL.PMUSERS - List of the outlets each user can access.
(e.g. Joe: 1-3; Jane: 4,5,6)

all.pmusers[#] :

ALL.PMOUTLET - The number of the outlet where the server is plugged.

all.pmoutlet[#] :

Screen 5:
********************************************************************************************************************
******** Configuration Wizard ********
********************************************************************************************************************

ALL.PMKEY - The hot-key that identifies the power management command.

all.pmkey[^p] :

ALL.PMNUMOFOUTLETS - The number of outlets you have on the AlterPath PM.

all.pmNumOfOutlets[8] :
Screen 6:
***********************************************************
*********** C O N F I G U R A T I O N   W I Z A R D ***********
***********************************************************

Current configuration:
(The ones with the '#' means it's not activated.)

all.protocol : ipdu
all.pmttype : cyclades
all.pmusers : #
all.pmoutlet : #
all.pmkey : ^p
all.pmNumOfOutlets : 8

Are these configuration(s) all correct (y/n) [n] :

How to Access the AlterPath PM regular menu from the Console Session

Step 1: Open a console session.
Open a telnet or ssh session for the serial port.

Step 2: Access the IPDU regular menu.
This should be done, for example, when the server crashes and it necessary to change the power status. Type the preconfigured hot-key.

If the user does not have permission to access any outlet, the following message will appear, and you will return to the Console Session:

It was impossible to start a Power Management Session
You can't access any Power Management functionality. Please contact your Console Server Administrator.
If the user does not have permission to access the outlet(s) of this server, but can access another outlet, the following message will appear:
You cannot manage the outlet(s) of this server.
Please enter the outlet(s) (or 'h' for help):

The user should type the outlet(s) he wants to manage, before reaching the main menu. The main menu will appear only if the user has permission for this/these outlet(s). Typing 'h' will cause the session to show text explaining what to type, and 'l' will cause the PM session to be logged out, and the user to return to the Console Session. If the user has permission to access the outlet(s) of this server, these outlets will be managed by the PM session.

Step 3: Regular Menu.

This is the AlterPath PM regular menu:

-------------------------------------------------------
Cyclades Corporation - Power Management Utility
-------------------------------------------------------
1 - Exit   2 - On   3 - Off
4 - Cycle  5 - Lock 6 - Unlock
7 - Status 8 - Help 9 - Other

Please choose an option:

Table 16: AlterPath PM Regular Menu Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exit</td>
<td>Exits the Power Management Session.</td>
</tr>
<tr>
<td>On</td>
<td>Turns the outlet on.</td>
</tr>
<tr>
<td>Off</td>
<td>Turns the outlet off.</td>
</tr>
<tr>
<td>Cycle</td>
<td>Turns the outlet off and back on.</td>
</tr>
<tr>
<td>Lock</td>
<td>Locks the current status of the outlet.</td>
</tr>
<tr>
<td>Unlock</td>
<td>Unlocks the current status of the outlet.</td>
</tr>
<tr>
<td>Status</td>
<td>Shows the current status of the outlet.</td>
</tr>
<tr>
<td>Other</td>
<td>Allows user to control other outlets.</td>
</tr>
</tbody>
</table>
**Step 4:** Check the status of the server's outlet or the outlet list.

Type '7' and wait for the answer. For example:

Please choose an option: 7

IPDU 1 Outlet 8:
Outlet Status User
8 OFF NONE

Cyclades Corporation - Power Management Utility

1 - Exit 2 - On 3 - Off
4 - Cycle 5 - Lock 6 - Unlock
7 - Status 8 - Help 9 - Other

Please choose an option:

**Step 5:** Reboot the server.

If the outlet(s) is/are locked, the user must unlock the outlet(s) first (option 6 - Unlock). The Cycle command turns the power off for some seconds and the turn it on again. Type '4' and wait for the answer. For example:

Please choose an option: 4

IPDU 1 Outlet 8:
8: Outlet power cycled.

Cyclades Corporation - Power Management Utility

1 - Exit 2 - On 3 - Off
4 - Cycle 5 - Lock 6 - Unlock
7 - Status 8 - Help 9 - Other

Please choose an option:
Chapter 3 - Additional Features

Step 6: Change the outlet list.

If the user needs to access another outlet(s) which can be managed by him, the option 9 - Other should be used. For example:

Cyclades Corporation - Power Management Utility

1 - Exit 2 - On 3 - Off
4 - Cycle 5 - Lock 6 - Unlock
7 - Status 8 - Help 9 - Other

Please choose an option: 9
Please enter the outlet(s) (or 'h' for help): 1.2

Cyclades Corporation - Power Management Utility

1 - Exit 2 - On 3 - Off
4 - Cycle 5 - Lock 6 - Unlock
7 - Status 8 - Help 9 - Other

Please choose an option:

From this point, all the commands will be related to the 2nd outlet of the IPDU in the port 1.

Step 7: Return to the Console Session.

The user can exit from the PM session and return to the Console Session in three ways:

1. Type the hot-key again, any time.
2. If the session is waiting for a menu option, type the option 1 - Exit.
3. If the session is waiting for the outlet, type 'l'.

When the user leaves the PM session, the following message will appear:

Exit from PM session
Chapter 3 - Additional Features

Power Management for the Authorized Users (firmware version prior to 1.4.0)

This section applies only for units not running firmware version 1.4.0 or greater. If you are running version 1.4.0 or greater please disregard this section, since it is not necessary to associate a special group for power management users. You just have to configure sXX.pmusers as described in “Port Slave Parameters Involved and Passed Values” on page 294.

The administrator or any user that belongs to the pmusers group, can log onto the Console server itself, and have total control over all the IPDU outlets. An additional menu, with more options than the regular menu, is provided for the administrator and users contained in the pmusers group to manage any IPDU.

There are two commands which can be used to manage the IPDU. The first one (pm) deals with menu options, while the second one (pmCommand) deals with the commands as they are sent to the IPDU, and requires more knowledge about the AlterPath-PM commands.

Adding an user of the pmusers group

Only the root user and users belonging to the pmusers group can do power management by using the pm or pmCommand. To add an user as member of the pmusers group, log in as “root” and run the ‘adduser’ command with the following syntax:

```
# adduser -g pmusers <username>
```

Changing the group of an already existing user

It is also possible to change the group of an already existing user. In this example we will change the groups of the already existing users: “cyclades” and “test”. To do that follow the steps below:

Step 1: Open the file /etc/group.

To open this file, run the command:

```
# vi /etc/group
```

Step 2: Addind the “cyclades” and “test” users to the pmusers group.

To change the group of these users, look for the line that begins with “pmusers”. At the end of this line, just after the ‘:’ character, insert the “cyclades” and “test” users.
Chapter 3 - Additional Features

webadmin::504:root
pmusers::505:cyclades,test
cyclades:x:506:
test:x:507:

Step 3: Save the configuration.
To save the changes done, run the command:

# saveconf

pm command
There are two ways to use this command: menu interface or command line. The menu is reached by typing the following command, from the prompt:

pm <IPDU port>

For example (menu for the root user):

------------------------------------------------------------------
Cyclades Corporation - Power Management Utility
------------------------------------------------------------------

Please choose an option:

Exit - Exits the Power Management session
On  - Turn outlet(s) ON
Off - Turn outlet(s) OFF
Cycle - Turn outlet(s) OFF and back ON
Lock - Lock the current status of outlet(s)
Unlock - Unlock the current status of outlet(s)
Chapter 3 - Additional Features

Status - Show the current status of outlet(s)
Interval - Sets/reads the power up interval
Name - Names an outlet
Current - Show current consumption for the entire unit
Temperature - Sets/reads/reset the temperature
Version - Displays version information
Who am I - Display the current username
Help - Shows this message
Buzzer - Turn buzzer on or off
Current Protection - Sets/reads the over current protection
Factory Default - Brings the unit to factory configuration
Reboot - Reboot the units in chain
Restore - Restore the configuration in flash
Save - Save configuration and status
Syslog - Turn syslog on or off
Alarm - Set alarm threshold for current
Password - Set a password for the specific user

Some of these options require the outlet number (On, Off, Cycle, Lock, Unlock, Status), and others don’t. In the first case, when the option is selected, the number of the outlet will be asked. The user can enter one or more outlets (separated by commas or dashes), or “all,” to apply the option to all the outlets.

Following are examples of some things which can be done through this command.

Turning the IPDU outlet 2 off

-----------------------------------------------
Cyclades Power Management Menu
PowerPort: pm10
-----------------------------------------------

Please choose an option: 3
Outlet name or outlet number(? for help, m for main menu): 2
Chapter 3 - Additional Features

Locking the outlets 1 to 3

When the outlet is locked, the previous status cannot be changed, until the outlet is unlocked. This means that if the outlet was on, it cannot be turned off and, if it was off, it cannot be turned on.

Cyclades Power Management Menu
PowerPort: pm10


Please choose an option: 5
Outlet name or outlet number(? for help, m for main menu): 1-3

Retrieving the status of the outlets

Cyclades Power Management Menu
PowerPort: pm10


Please choose an option: 7
Outlet name or outlet number(all for all, ? for help, m for main menu): 8

<table>
<thead>
<tr>
<th>Outlet</th>
<th>Name</th>
<th>Status</th>
<th>Users</th>
<th>Interval (s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td></td>
<td>Unlocked ON</td>
<td></td>
<td>0.50</td>
</tr>
</tbody>
</table>
**Chapter 3 - Additional Features**

**pmCommand command**

Through pmCommand command, the administrator has access to other options beyond the menu options, because he will be accessing the IPDU itself. The administrator must have a good knowledge of the AlterPath PM command set to use it.

There are two ways to use this command. If only the IPDU port is passed as an argument, it will appear in a prompt where the administrator can write the command. Otherwise, the arguments after the IPDU port will be considered the PM command.

Syntax:

```
pmCommand <IPDU port> [<command>]
```

For example:

```
[root@CAS root]# pmCommand 1
You're entering the "Power Management Prompt".
To go back to the Console Server's command line type: exitPm
```

```
[Cyclades - Power Management Prompt]#
```

The following are examples of some things which can be done through this command.

**Listing the commands available for the AlterPath PM**

```
[Cyclades - Power Management Prompt]# help
```

- `on <outlet><cr>` -- Turn `<outlet>` ON
- `off <outlet><cr>` -- Turn `<outlet>` OFF
- `cycle <outlet><cr>` -- Turn `<outlet>` OFF and back ON
- `lock <outlet><cr>` -- Lock the current status of `<outlet>`
- `unlock <outlet><cr>` -- Unlock the current status of `<outlet>`
- `status <outlet><cr>` -- Show the current status of `<outlet>`
- `list<cr>` -- List users created and eventual outlets assigned
- `exit<cr>` -- Exit session
- `passwd <user><cr>` -- Set a password for the specific user
- `help<cr>` -- Show supported commands
- `current<cr>` -- Show the instantaneous current consumption for the entire unit
- `adduser <username><cr>` -- Add user to the DB (8 maximum users
allowed)
deluser <username><cr> --Delete user from the DB
assign <outlet><username><cr> --Assign <outlet> to a specific user
name <outlet> <name><cr> --Name an outlet
[Cyclades - Power Management Prompt]#

Cycling all the outlets
[Cyclades - Power Management Prompt]# cycle all

1: Outlet power cycled.
2: Outlet power cycled.
3: Outlet power cycled.
4: Outlet power cycled.
5: Outlet power cycled.
6: Outlet power cycled.
7: Outlet power cycled.
8: Outlet power cycled.
[Cyclades - Power Management Prompt]#

Unlocking the outlets 1, 5 and 8
[Cyclades - Power Management Prompt]# unlock 1, 5, 8

1: Outlet unlocked.
5: Outlet unlocked.
8: Outlet unlocked.

Turning the outlet off
[Cyclades - Power Management Prompt]# off 2

2: Outlet turned off.
Chapter 3 - Additional Features

AlterPath PM Firmware Upgrade

It is possible to upgrade the firmware of the IPDU unit connected to any serial port of the Cyclades-TS. It is also possible to upgrade the whole daisy-chain of AlterPath PM units, since the unit(s) before the targeted one has firmware version 1.2.2 or greater.

Upgrade Process

To upgrade the firmware of the PM units follow the steps below:

**Step 1: Download the firmware.**

The first step of the upgrade process will be the download of the new firmware. Cyclades provides a directory on its ftp site where it is possible to check for new firmwares and download them to the Cyclades-TS. It is recommended to download the new firmware to the /tmp directory because files in this directory are deleted during the boot process.

**Step 2: Run the pmfwupgrade application.**

After downloading it is necessary to call an application called *pmfwupgrade*. This application has the following syntax:

```
# pmfwupgrade [-h] [-f] [-F] [-v] <serial port number>[:<unit number>] <filename>
```

where:

- `-h` = Show the help message and exit
- `-f` = The upgrade is done without asking any questions
- `-F` = The upgrade is done without waiting logical connection with the AlterPath PM. This is should be used after possible power failure during the upgrade process.
- `-v` = show messages about the status of the upgrade.

`<serial port number>` = the serial port where the PM unit is connected

`[:<unit number>]` = number of the PM unit when in daisy-chain. If is not used, all units in the serial port will have the firmware upgraded, when possible

`<filename>` = complete path of the file that has the PM firmware (default: /tmp/pmfirmware)
Chapter 3 - Additional Features

**Important!** If the AlterPath PM unit is not configured with the default password, it will be necessary to inform it to the Cyclades-TS by editing the `/etc/pm.cyclades` file and changing the parameter `admPasswd` with the correct password.

The `pmfwupgrade` application will try to stop all the process that are using the serial port. Just type YES to proceed into the upgrade process. Another message will prompt asking for confirmation to proceed with the upgrade process. Type ‘y’ to upgrade the PM unit firmware.

**Warning!** Depending on the hardware version of the AlterPath PM, it is possible that all outlets completely powers off during the upgrade process. Make sure to shutdown all devices connected to them before starting the firmware upgrade process.
Chapter 3 - Additional Features

Power Management from a Browser

The Console Server Web server also supports power management. From a Web browser it is possible to check the status of all the IPDUs connected to the Console Server, as well as their outlets. If the user has Administration privileges, he can also perform the commands to turn on, turn off, cycle, lock and unlock the outlets.

**Step 1:** Point your browser to the Console Server.
In the address or location field of your browser type the Console Access Server's IP address. For example:

http://10.0.0.0

**Step 2:** Log in as root and type the Web root password configured by the Web server.
This will take you to the Configuration and Administration page.

**Step 3:** Select the Power Management link.
This link is in the Administration section. The following page will appear:

![Figure 34: Power Management page](image)

User Guide 313
Chapter 3 - Additional Features

In the figure above, all the outlets are off (the light bulbs are off) and unlocked. For this status, there are two possible commands: turn it on and lock it.

The following steps are examples of what can be done in this page.

**Step 4: Turn the outlet 1 on.**
Click on the “On 48:1” button. The following page will appear:

<table>
<thead>
<tr>
<th>Serial Port</th>
<th>Description</th>
<th>Outlets</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Type: cyclades</td>
<td></td>
</tr>
<tr>
<td>outlet 1</td>
<td>Status: Detected</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Number</th>
<th>Serial Port</th>
<th>Status</th>
<th>Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>None</td>
<td>Off 48.1</td>
<td>Cycle 48.1</td>
</tr>
<tr>
<td>2</td>
<td>None</td>
<td>On 48.2</td>
<td>Lock 48.2</td>
</tr>
<tr>
<td>3</td>
<td>None</td>
<td>On 48.3</td>
<td>Lock 48.3</td>
</tr>
<tr>
<td>4</td>
<td>None</td>
<td>On 48.4</td>
<td>Lock 48.4</td>
</tr>
<tr>
<td>5</td>
<td>None</td>
<td>On 48.5</td>
<td>Lock 48.5</td>
</tr>
<tr>
<td>6</td>
<td>None</td>
<td>On 48.6</td>
<td>Lock 48.6</td>
</tr>
<tr>
<td>7</td>
<td>None</td>
<td>On 48.7</td>
<td>Lock 48.7</td>
</tr>
<tr>
<td>8</td>
<td>None</td>
<td>On 48.8</td>
<td>Lock 48.8</td>
</tr>
</tbody>
</table>

*Figure 35: Power Management page after turning outlet 1 on*

After this operation, the outlet 1 was turned on (the light bulb is on), and now the administrator can turn it off and cycle this outlet.

**Step 5: Lock outlet 1.**
Click on the “Lock 48:1” button. The following page will appear:
## Chapter 3 - Additional Features

### Figure 36: Power Management page after locking outlet 1

The padlock indicates that outlet 1 was locked. From this point, nothing can change the outlet status, until the outlet is unlocked.

<table>
<thead>
<tr>
<th>Serial Port</th>
<th>Description</th>
<th>Outlets</th>
</tr>
</thead>
<tbody>
<tr>
<td>My48</td>
<td>Type: cyclical&lt;br&gt;Outlets: 8&lt;br&gt;Status: Detected</td>
<td>Number</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5</td>
</tr>
<tr>
<td></td>
<td></td>
<td>6</td>
</tr>
<tr>
<td></td>
<td></td>
<td>7</td>
</tr>
<tr>
<td></td>
<td></td>
<td>8</td>
</tr>
</tbody>
</table>
Menu Shell

The menu shell feature allows a user to be presented with a menu in order to connect to a set of hosts as defined by the Cyclades-TS administrator. It can be used as an easy method for users to access servers on the LAN.

How to use
Once the appropriate configurations are done the user will connect to the Cyclades-TS using a serial terminal. The user will then automatically receive a menu similar to that shown below:

Welcome!

1) Sun server
2) Dell server
3) Linux server
4) Quit

Option =>

The user selects the option required to connect to the desired server or to exit the system.

How to configure

Setting up the menu - from the command line

Step 1: Type "menush_cfg" and use the options shown below to define the menu title and menu commands.

-------------------------------------------------
MenuShell Configuration Utility
-------------------------------------------------

Please choose from one of the following options:

1. Define Menu Title
Chapter 3 - Additional Features

2. Add Menu Option
3. Delete Menu Option
4. List Current Menu Settings
5. Save Configuration to Flash
6. Quit

Option =>

Accessing the menu - VI mode

To configure which ports will prompt the menu shell and if it will require authentication to gain access to it, follow the steps below:

Step 1: If no authentication is required to gain access to the menu.

Configure the following parameters in /etc/portslave/pslave.conf for the ports that will use this menu shell.

s<x>.protocol  telnet
conf.telnet   /bin/menush
s<x>.authtype  none

Where  <x> is the port number being configured.

Step 2: If authentication is required to gain access to the menu.

The user's default shell must be modified to run the /bin/menush. So in /etc/passwd the shell should be changed as follows. There should be something like:

user:FrE6QU:505:505:Embedix User,,,:/home/user:/bin/menush

In pslave.conf the port where the serial terminal is attached must be configured for login with authentication local. Configure the following lines:

s<x>.protocol login
s<x>.authtype local

Where  <x> is the port number being configured.
Chapter 3 - Additional Features

The SNMP Proxy for Power management feature allows the Cyclades-TS console servers to proxy SNMP requests to the Cyclades Intelligent Power Distribution Units. This allows SNMP clients to query and control the remote IPDU using standard set and get commands.

How to Configure

You should ensure that the AlterPath PM is correctly installed and configured by following the procedure outlined in the Power Management Appendix of this user Manual. You must also ensure that SNMP is correctly configured by following the configuration instructions in Chapter 3 - SNMP.

The parameters and features that can be controlled in the remote IPDU are as follows:-

- The number AlterPath PM units connected to a given console server
- The number of the outlets connected to a given port
- The number the AlterPath PM units connected to this port (when a daisy chain configuration is being used).
- The instantaneous RMS current being drawn from each of the AlterPath PM unit(s) connected to this port.
- The software version of the AlterPath PM unit(s) connected to this port
- The temperature of the AlterPath PM unit(s) connected to this port
- The name of the outlet as configured in the AlterPath PM.
- The alias of the server that is configured as using this outlet
- The name of the serial console connection that corresponds to the host which this outlet controls power.
- The status of the outlet
  - power status : 0 (off), 1 (on), 3 (unknow)
  - lock state : 0 (unlock), 1 (lock), 2 (unknow)

This feature will allow the user to control the AlterPath PM outlets using SNMP set commands. These following actions will be allowed to each outlet by this feature :
1) ON
2) OFF
Chapter 3 - Additional Features

3) CYCLE
4) LOCK
5) UNLOCK

Important! The Cyclades-TS proxies all SNMP requests to the AlterPath PM unit. Therefore there is a small delay if an outlet cycling is requested by the snmpset command. To successfully cycle an outlet, a 4 second or higher timeout must be specified. To run this command for more than one outlet or for units configured as daisy chain, this time should be recalculated.

Examples:

This feature allows the user do these following SNMP requests:

1) get the number of Cyclades-TS serial ports that has PM connected to:

   # snmpget -m all -v 2c -t 4 -c cyclades 10.10.0.1 .cyNumberOfPM <enter>

   enterprises.cyclades.cyACSMgmt.cyPM.cyNumberOfPM.0 = 2

2) get the number of outlets of the PM connected to serial port 16:

   # snmpget -m all -v 2c -t 4 -c cyclades 10.10.0.1 .cyPMNumberOutlets.16 <enter>

   enterprises.cyclades.cyACSMgmt.cyPM.cyPMtable.cyPMEntry.cyPMNumberOutlets.16 = 8

3) get the number of units of the PM connected to serial port 14:

   # snmpget -m all -v 2c -t 4 -c cyclades 10.10.0.1 .cyPMNumberUnits.14 <enter>

   enterprises.cyclades.cyACSMgmt.cyPM.cyPMtable.cyPMEntry.cyPMNumberUnits.14 = 2

For more examples and MIB definition please search the online FAQ at:
www.cyclades.com/support/faqs.php
Chapter 3 - Additional Features

Start and Stop Daemons

This feature allows daemons (services) to be enabled or disabled without need of reboot the Cyclades-TS. A simple engine detects configuration changes (file comparison). This feature is implemented with shell scripts. There is one main shell script called `daemon.sh` and one sourced shell script (included by daemon.sh) for every daemon (service) that runs in the Cyclades-TS. The shell script daemon.sh must be run once by inittab and every time a configuration change is made. The daemon.sh reads a file `/etc/daemon_list` which contains the names of all sourced shell scripts and performs the start/stop/restart operation needed if any file related to service was changed. The daemon.sh will keep a hidden copy, prefixed with "." and suffixed with `.tmp`, of all related files in the directory `/var/run`.

Each sourced shell script has a set of mandatory shell variables handled directly by the shell script daemon.sh. The sourced shell scripts may have other shell variables not handled directly by daemon.sh. Such variables have the sole purpose of facilitating the configuration of command line parameters.

The mandatory shell variables define:

1. If the service is enabled or disabled. (ENABLE=YES/NO)
2. The pathname to the daemon. (DNAME=<daemon name, DPATH=<daemon path>)
3. How to restart the daemon: by signal (kill, hup, term, etc) or by command (start, stop, etc). (DTYPE=sig/cmd)
4. Signal to be sent to the daemon. Default is `term`. (DSIG=<signal>)
5. A list of configuration files. The files in this list will be checked for changes. (ConfigFiles=<config file list>)
6. A initialization shell script that will be run before start the service. (ShellInit=<shell_script_name [command line parameters]>)
7. Command line parameters to start the daemon. (DPARM=<command line parameters>)
8. Command Line parameters to stop the daemon. (DSTOP=<command line parameters>)

The daemon.sh may be executed in two ways:
Chapter 3 - Additional Features

1. Without parameters in the command line, it will check the configuration files of the service and restart or stop it if needed.

2. It will perform the requested action (stop/restart) in the list of services given in the command line regardless any configuration changes.

The command `daemon.sh help` will display a list of services available. Currently the following services are handled by daemon.sh. The first column is the service ID, the second is the name of the shell script file.

<table>
<thead>
<tr>
<th>Service</th>
<th>Configuration File</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NTP</td>
<td>/etc/ntpclient.conf</td>
<td>// Network Timer client</td>
</tr>
<tr>
<td>SNMP</td>
<td>/etc/snmpd.conf</td>
<td>// SNMP</td>
</tr>
<tr>
<td>SYSLOG</td>
<td>/etc/syslog.sh</td>
<td>// Syslog daemon</td>
</tr>
<tr>
<td>SSH</td>
<td>/etc/sshd.sh</td>
<td>// Secure shell</td>
</tr>
<tr>
<td>INETD</td>
<td>/etc/inetd.sh</td>
<td>// Network services daemon</td>
</tr>
<tr>
<td>PMD</td>
<td>/etc/pmd.sh</td>
<td>// Power Management daemon</td>
</tr>
</tbody>
</table>

The following example will stop power management, ssh and network timer client services.

`daemon.sh PMD SSH NTP stop`
Chapter 3 - Additional Features

How to Configure Them

Example of sourced shell script that activates the ntpclient service (type sig).

# This file defines the NTP client configuration
ENABLE=NO         # Must be "NO" or "YES" (uppercase)
DNAME=ntpclient   # daemon name
DPATH=/bin        # daemon path
ShellInit=        # Performs any required initialization
ConfigFiles=      # configuration files
DTYPE=sig         # must be "sig" or "cmd" (lowercase)
DSIG=kill         # signal to stop/restart the daemon (lowercase)
# if it's hup term will be used to stop the daemon
# daemon command line parameters
NTPSERVER="-h 129.6.15.28"  # NTP server ip address
NTPINTERVAL="-l 300"        # Time in seconds to ask server
NTPCOUNT="-c 0"            # counter : 0 means forever
DPARM="$NTPCOUNT $NTPSERVER $NTPINTERVAL"
DSTOP=

Example of sourced shell script that activates the ipsec service (type cmd).

# This file defines the ipsec configuration
ENABLE=NO         # Must be "NO" or "YES" (uppercase)
DNAME=ipsec       # daemon name
DPATH=/usr/local/sbin        # daemon path
ShellInit=/etc/ipsec.init    # Performs any required initialization
Chapter 3 - Additional Features

ConfigFiles=          # configuration files
DTYPE=cmd            # must be "sig" or "cmd"
DSIG=kill            # signal to stop/restart the daemon (lowercase)
                      # if it's hup term will be used to stop the daemon
                      # daemon command line parameters
DPARM="setup --start"
DSTOP="setup --stop"
Chapter 3 - Additional Features

This page has been left intentionally blank.
Appendix A - New User Background Information

Users and Passwords

A username and password are necessary to log in to the Cyclades-TS. The user root is predefined, with a password tslinux. A password should be configured as soon as possible to avoid unauthorized access. Type the command:

passwd

to create a password for the root user. To create a regular user (without root privileges), use the commands:

adduser user_name

passwd user_password

To log out, type “logout” at the command prompt.

A regular user who wants to run the command su - to become a superuser needs to:

Step 1: Make sure the group wheel is already created.
An administrator with root access would run the following command:

addgroup wheel

In file /etc/group there should be a line with at least the following:

wheel::zzz:

Step 2: Belong to the group wheel.
An administrator with root access would edit /etc/group file and insert the username at the end of the wheel line. For example, for user steve, the administrator would edit the line in file/etc/group:

wheel::zzz:

to add "steve" at the end like this:

wheel::zzz:steve
Appendix A - New User Background Information

How to show who is logged in and what they are doing

The command “w” displays information about the users currently on the machine, and their processes. It calls two commands: w_ori and w_cas. The w_ori is the new name of the original command “w” and the w_cas shows the CAS sessions information.

The header of w_ori shows, in this order: the current time, how long the system has been running, how many users are currently logged on (excluded the CAS users), and the system load averages for the past 1, 5, and 15 minutes.

The following entries are displayed for each user (excluded the CAS users): login name, the tty name, the remote host, login time, idle time, JCPU time (it is the time used by all processes attached to the tty), PCPU time (it is the time used by the current process, named in the “what” field), and the command line of their current process.

The header of w_cas shows how many CAS users are currently logged on. The following entries are displayed for each CAS user: login name, the tty name, the remote host and remote port, login time, the process ID and the command line of the current process.

Linux File Structure

The Linux file system is organized hierarchically, with the base (or root) directory represented by the symbol “/”. All folders and files are nested within each other below this base directory. The directories located just below the base directory are:

- `/home` Contains the work directories of system users.
- `/bin` Contains applications and utilities used during system initialization.
- `/dev` Contains files for devices and ports.
- `/etc` Contains configuration files specific to the operating system.
- `/lib` Contains shared libraries.
- `/proc` Contains process information.
Appendix A - New User Background Information

/mnt Contains information about mounted disks.
/opt Location where packages not supplied with the operating system are stored.
/tmp Location where temporary files are stored.
/usr Contains most of the operating system files.
/var Contains operating system data files.

Basic File Manipulation Commands

The basic file manipulation commands allow the user to copy, delete, and move files and create and delete directories.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
</table>
| cp file_name destination | Copies the file indicated by file_name to the path indicated by destination. | a) cp text.txt /tmp  
b) cp /chap/robo.php ./excess.php |
| rm file_name | Removes the file indicated by file_name. |  |
| mv file_name destination | Moves the file indicated by file_name to the path indicated by destination. |  |
| mkdir directory_name | Creates a directory named directory_name. | a) mkdir spot  
b) mkdir /tmp/snuggles |
| rmdir directory_name | Removes the directory indicated by directory_name. |  |

Other commands allow the user to change directories and see the contents of a directory.
Appendix A - New User Background Information

pwd Supplies the name of the current directory. While logged in, the user is always “in” a directory. The default initial directory is the user's home directory: /home/<username>

ls [options] directory_name Lists the files and directories within directory_name. Some useful options are -l for more detailed output and -a which shows hidden system files.

cd directory_name Changes the directory to the one specified.

cat file_name Prints the contents of file_name to the screen.

Shortcuts:

. (one dot) Represents the current directory.

.. (two dots) Represents one directory above the current directory (i.e. one directory closer to the base directory).

The vi Editor

To edit a file using the vi editor, type:

vi file_name

Vi is a three-state line editor: it has a command mode, a line mode and an editing mode. If in doubt as to which mode you are in, press the <ESC> key which will bring you to the command mode.
When you enter the vi program, you are automatically in command mode. To navigate to the part of the file you wish to edit, use the following keys:

**Table 18: vi navigation commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$b$</td>
<td>Moves the cursor to the left</td>
</tr>
<tr>
<td>$j$</td>
<td>Moves the cursor to the next line</td>
</tr>
<tr>
<td>$k$</td>
<td>Moves the cursor to the previous line</td>
</tr>
<tr>
<td>$l$</td>
<td>Moves the cursor to the right</td>
</tr>
</tbody>
</table>

Having arrived at the location where text should be changed, use these commands to modify the text (note commands “i” and “o” will move you into edit mode and everything typed will be taken literally until you press the <ESC> key to return to the command mode).
Appendix A - New User Background Information

Table 19: vi file modification commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>i</code></td>
<td>Inserts text before the cursor position (everything to the right of the cursor is shifted right).</td>
</tr>
<tr>
<td><code>o</code></td>
<td>Creates a new line below the current line and insert text (all lines are shifted down).</td>
</tr>
<tr>
<td><code>dd</code></td>
<td>Removes the entire current line.</td>
</tr>
<tr>
<td><code>x</code></td>
<td>Deletes the letter at the cursor position.</td>
</tr>
</tbody>
</table>

After you have finished modifying a file, enter line mode (by typing “:” from command mode) and use one of the following commands:

Table 20: vi line mode commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>w</code></td>
<td>Saves the file (w is for write).</td>
</tr>
<tr>
<td><code>wq</code></td>
<td>Saves and closes the file (q is for quit).</td>
</tr>
<tr>
<td><code>q!</code></td>
<td>Closes the file without saving.</td>
</tr>
<tr>
<td><code>w file</code></td>
<td>Saves the file with the name <code>&lt;file&gt;</code>.</td>
</tr>
<tr>
<td><code>e file</code></td>
<td>Opens the file named <code>&lt;file&gt;</code>.</td>
</tr>
</tbody>
</table>
The Cyclades-TS has a static routing table that can be seen using the commands:

```
route
or
netstat -rn
```

The file `/etc/network/st_routes` is the Cyclades-TS's method for configuring static routes. Routes should be added to the file (which is a script run when the Cyclades-TS is initialized) or at the prompt (for temporary routes) using the following syntax:

```
```

- `[add|del]` One of these tags must be present. Routes can be either added or deleted.
- `[-net|-host]` Net is for routes to a network and -host is for routes to a single host.
- `target` Target is the IP address of the destination host or network.
- `netmask` The tag `netmask` and `nt_mask` are necessary only when subnetting is used, otherwise, a mask appropriate to the target is assumed. `nt_msk` must be specified in dot notation.
- `gw gt_way` Specifies a gateway, when applicable. `gt_way` is the IP address or hostname of the gateway.
- `interf` The interface to use for this route. Must be specified if a gateway is not. When a gateway is specified, the operating system determines which interface is to be used.
Secure Shell Session

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 Cyclades-TS offers both. The command to start an ssh client session from a UNIX workstation is:

```
ssh -t <user>@<hostname>
```

where

```
<user> = <username>:ttySnn or
     <username>:socket_port or
     <username>:ip_addr or
     <username>:serverfarm
```

Note: “serverfarm” is a physical port alias. It can be configured in the file pslave.conf.
An example:

```
username: cyclades
TS1000 IP address: 192.168.160.1
host name: ts1000
servername for port 1: file_server
```

ttyS1 is addressed by IP 10.0.0.1 or socket port 7001. The various ways to access the server connected to the port are:

```
ssh -t cyclades:ttyS1@ts1000
ssh -t cyclades:7001@ts1000
ssh -t cyclades:10.0.0.1@ts1000
ssh -t cyclades:file_server@ts1000
```
Appendix A - New User Background Information

ssh -t -l cyclades:10.0.0.1ts1000
ssh -t -l cyclades:7001 ts1000

For openssh clients, version 3.1p1 or later ssh2 is the default. In that case, the -1 flag is used for ssh1.

ssh -t cyclades:7001@ts1000
(Openssh earlier than 3.1p1 - Cyclades-TS V_1.3.1 and earlier -> ssh1 will be used)

ssh -t -2 cyclades:7001@ts1000
(Openssh earlier than 3.1p1 - Cyclades-TS V_1.3.1 and earlier -> ssh2 will be used)

ssh -t cyclades:7001@ts1000
(Openssh 3.1p1 or later - Cyclades-TS V_1.3.2 or later/AlterPath Console Server version 2.1.0 or later -> ssh2 will be used)

ssh -t -1 cyclades:7001@ts1000
(Openssh 3.1p1 or later - Cyclades-TS V_1.3.2 or later/ssh1 will be used)

To log in to a port that does not require authentication, the username is not necessary:

ssh -t -2 :ttyS1@ts1000

Note: In this case, the file sshd_config must be changed in the following way:

PermitRootLogin Yes
PermitEmptyPassword Yes
Appendix A - New User Background Information

The Session Channel Break Extension
This is a new feature for the AlterPath Console Server version 2.1.3 and Cyclades-TS version 1.3.7. The Cyclades-TS provides new way to send a break signal during a SSH version 2 terminal session. This method is defined by “Session Channel Break Extension : draft-ietf-secsh-break-00.txt.” In previous Cyclades-TS versions there is one break lenght in milliseconds (break duration). Now the Cyclades-TS have a new parameter <all/Sx>.break_interval, which is used with all.break_sequence (<all/Sxx>.break_sequence). (This improves the SSH-break Cyclades implementation).

The ssh2-client receives a command ("<ssh escape char>B") from the user and sends one "break request" to ssh-server. The ssh-server receives the "break request" and sends a break command to the serial port. The ssh client can send the break duration (break interval), so the user can configure this value by command line ("-B <break interval in miliseconds>") or by ssh_config file ("breakinterval <break interval in miliseconds>").

How it works in SSH Server (all.protocol is socket_ssh)
The serial driver accepts the parameter break interval in the break command. If the version is 2 (ssh-2), the server accepts and treats the "break request" sent by the client. The "break request" defines the break-length in miliseconds. The server sends a break command with the break-length to the serial driver to perform the break in the serial port. If the parameter all.break_sequence is configured and the server finds the sequence in the data received from client, the server sends a break command with all.break_interval to serial driver.

How it works in SSH Client
The SSH client has a new option ".B <break_interval in miliseconds>" and accepts break_interval in ssh_config. When the user types "<ssh-escape>B" (where ssh-escape is ~") the client sends a "break request" to ssh-server. When the Cyclades-TS calls the ssh-client automatically, it uses the parameter all.break_interval to calls the ssh-2 client.

Configuring sshd's client authentication using SSH Protocol version 1

Step 1: Only RhostsAuthentication yes in sshd_config.
In the linux host enable in the file /etc/ssh/sshd_config the parameters:

Host *

RhostsAuthentication yes
Appendix A - New User Background Information

UsePrivilegedPort yes

- One of these:

hostname or ipaddress in /etc/hosts.equiv or /etc/ssh/shosts.equiv

hostname or ipaddress and username in ~/.rhosts or ~/.shosts and IgnoreRhosts no in sshd_config

- Client start-up command: ssh -t <TS_ip or Serial_port_ip> (if the ssh client is running under a session belonging to a username present both in the workstation’s database and the TS’s database).

- Client start-up command: ssh -t -l <username> <TS_ip or Serial_port_ip> (if the ssh client is running under a session belonging to a username present only in the workstation’s database. In this case, the <username> indicated would have to be a username present in the TS’s database).

Note: For security reasons, some ssh clients do not allow just this type of authentication. To access the serial port, the TS must be configured for local authentication. No root user should be used as username.

Step 2: Only RhostsRSAAuthentication yes in sshd_config.

- One of the RhostsAuthentication settings, described in Step 1.

- Client machine’s host key ($ETC/ssh_host_key.pub) copied into the T/tmp/known_hosts file. The client hostname plus the information inside this file must be appended in one single line inside the file /etc/ssh/ ssh_known_hosts or ~/.ssh/known_hosts and IgnoreUserKnownHosts no inside sshd_config. The following commands can be used for example:

  echo 'n 'client_hostname ' >> /etc/ssh/ssh_known_hosts or ~/.ssh/known_hosts

  cat /tmp/known_hosts >> /etc/ssh/ssh_known_hosts or ~/.ssh/known_hosts

- client start-up command: ssh -t <TS_ip or Serial_port_ip>
Appendix A - New User Background Information

Step 3: Only RSAAuthentication yes in sshd_config.

- Removal of the TS's *.equiv, ~/.?hosts, and *known_hosts files.
- Client identity created by ssh-keygen and its public part (~/.ssh/identity.pub) copied into TS's ~/.ssh/authorized_keys.
- Client start-up command: ssh -t <TS_ip or Serial_port_ip>.

Step 4: Only PasswdAuthentication yes in sshd_config.

- Removal of the TS's *.equiv, ~/.?hosts, *known_hosts, and *authorized_keys files.
- Client startup command: ssh -t -l <username> <TS_ip or Serial_port_ip> or ssh -t -l <username:alias><TS_ip>.

Configuring sshd's client authentication using SSH Protocol version 2

Only PasswdAuthentication yes in sshd_config DSA Authentication is the default. (Make sure the parameter PubkeyAuthentication is enabled.)

- Client DSA identity created by ssh-keygen -d and its public part (~/.ssh/id_dsa.pub) copied into the TS's ~/.ssh/authorized_keys2 file.
- Password Authentication is performed if DSA key is not known to the TS. Client start-up command: ssh -2 -t <TS_ip or Serial_port_ip>.

Note: All files “~/*” or “~/.ssh/*” must be owned by the user and readable only by others. All files created or updated must have their full path and file name inside the file config_files and the command saveconf must be executed before rebooting the TS.
Appendix A - New User Background Information

Configuring the Session Channel Break Extension in SSH Server

**Step 1:** Configure the parameter **break_interval in pslave.conf.**
This can be done by the admin using the Web, snmpset, the Wizard or CLI.

**Step 2:** Configure the parameter **ssh_interval in ssh_config.**
This can be done using the vi editor.

## The Process Table

The process table shows which processes are running. Type `ps -a` to see a table similar to that below:

**Table 21: Process table**

<table>
<thead>
<tr>
<th>PID</th>
<th>UID</th>
<th>State</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>root</td>
<td>S</td>
<td>/sbin/inetd</td>
</tr>
<tr>
<td>31</td>
<td>root</td>
<td>S</td>
<td>/sbin/sshd</td>
</tr>
<tr>
<td>32</td>
<td>root</td>
<td>S</td>
<td>/sbin/cy_ras</td>
</tr>
<tr>
<td>36</td>
<td>root</td>
<td>S</td>
<td>/sbin/cy_wdt_led wdt led</td>
</tr>
<tr>
<td>154</td>
<td>root</td>
<td>R</td>
<td>/ps -a</td>
</tr>
</tbody>
</table>

To restart the cy_ras process use its process ID or execute the command:

```
signal_ras hup
```

This executes the ps command, searches for the cy_ras process id, then sends the signal `hup` to the process, all in one step. Never kill cy_ras with the signals -9 or SIGKILL.
Appendix A - New User Background Information

TS Menu Script

The ts_menu script can be used to avoid typing long telnet or ssh commands. It presents a short menu with the names of the servers connected to the serial ports of the Cyclades-TS. The server is selected by its corresponding number. ts_menu must be executed from a local session: via console, telnet, ssh, dumb terminal connected to a serial port, etc. Only ports configured for console access (protocols socket_server or socket_ssh) will be presented. To start having familiarity with this application, run ts_menu - h:

The meaning of each argument is:

- `-u<user>` - Invokes ts_menu as the user named by `<user>`. This requires a password to be entered.

- `-l[c]` - Generates a list of all ports that the user has access to and terminates. Port aliases will be presented if defined. For the remote ports (clustering) if port alias is not defined they will be shown as "ip_addr:port" (ip_addr referring to the slave ACS). The default is displaying ports in alphabetical order, but in case "c" flag is also specified the listing will be sorted by console server (master unit showing first).

- `-ro` - Invokes ts_menu in read only mode. It works even if the user is the only one logged to a certain port. In this mode, the user can connect to any port he has access to but cannot type in. He is in sniff mode. A message stating "Read only mode" is provided in case the user attempts to interact with that port. Note however that a real sniff session (the user isn't the first one to log to a certain port) is only allowed if he is authorized to.

- `-s` - Invokes ts_menu in a way that all ports (including slave ACSs) are presented in a single list sorted in alphabetical order. Not using this option causes the display to be as for the old implementation.

- `-auth` - For backward compatibility, this option makes the new ts_menu implementation behave as the old one so that authentication is performed again to access each port.

- `<console port>` - If issued, produces a direct connection to that port. In the case the user doesn't have access to that port or the port doesn't exist, the application returns a "console not found" message and terminates. `<console port>` can be the port alias or the port number. In case of clustering, port number must include a reference to the slave ACS as "host:port" (where host is the slave hostname or IP address).
Other options:

- **-p** - Display Tcp port
- **-i** - Display Local Ip assigned to the serial port
- **-u <name>** - Username to be used in ssh/telnet command
- **-U** - Always ask for an username
- **-e <[^\]char>** - Escape char used by telnet or ssh

Example:

```bash
> ts_menu
Master and Slaves Console Server Connection Menu
1 TSJen800
2 edson-r4.Cyclades.com
3 az84.Cyclades.com
4 64.186.190.85
5 az85.Cyclades.com

Type 'q' to quit, a valid option [1-5], or anything else to refresh:
```

By selecting 1 in this example, the user will access the local serial ports on that Cyclades-TS. If the user selects 2 through 5, remote serial ports will be accessed. This is used when there is clustering (one Cyclades-TS master box and one or more Cyclades-TS slave boxes).

If the user selects 1, the following screen is displayed:

```
Serial Console Server Connection Menu for your Master Terminal Server
1 ttyS1 2 ttyS2 3 s3serverfarm

Type 'q' to quit, 'b' to return to previous menu, a valid option[1-3], or anything else to refresh:
```
Appendix A - New User Background Information

Options 1 to 3 in this case are serial ports configured to work as a CAS profile. Serial port 3 is presented as an alias name (s3serverfarm). When no name is configured in pslave.conf, ttyS<N> is used instead. Once the serial port is selected, the username and password for that port (in case there is a per-user access to the port and -U is passed as parameter) will be presented, and access is granted.

To access remote serial ports, the presentation will follow a similar approach to the one used for local serial ports.

The ts_menu script has the following line options:

-p : Displays Ethernet IP Address and TCP port instead of server names.

Cyclades-TS: Serial Console Server Connection menu
1 209.81.55.79 7001 2 209.81.55.79 7002 3 209.81.55.79 7003
4 209.81.55.79 7004 5 209.81.55.79 7005 6 209.81.55.79 7006
Type 'q' to quit, a valid option [1-6], or anything else to refresh :

-i : Displays Local IP assigned to the serial port instead of server names.

Cyclades-TS: Serial Console Server Connection menu
1 192.168.1.101 2 192.168.1.102 3 192.168.1.103 4 192.168.1.104
5 192.168.1.105 6 192.168.1.106
Type 'q' to quit, a valid option [1-6], or anything else to refresh :

-u <name> : Username to be used in the ssh/telnet command. The default username is that used to log onto the Cyclades-TS.

-h : Lists script options.
Appendix A - New User Background Information
Appendix A - New User Background Information
Appendix B - Cabling, Hardware, & Electrical

General Hardware Specifications

The power consumption and heat dissipation, environmental conditions and physical specifications of the Cyclades-TS are listed below.

Table 23: Cyclades-TS power requirements

<table>
<thead>
<tr>
<th>Power Specifications</th>
<th>TS110/100</th>
<th>TS400</th>
<th>TS800</th>
<th>TS1000</th>
<th>TS2000</th>
<th>TS3000</th>
</tr>
</thead>
<tbody>
<tr>
<td>Input Voltage Range</td>
<td>External Universal Input Desktop Power Supply, 100-240VAC auto-range input, 5VDC output (Internal power modules available for 12VDC, 24VDC, -48VDC and Power Over Ethernet)</td>
<td>External Universal Input Desktop Power Supply (100-240VAC auto-range input, 5VDC output)</td>
<td>Internal 100-240VAC autorange (-48VDC option available)</td>
<td>Internal 100-240VAC autorange (-48VDC option available)</td>
<td>Internal 100-240VAC autorange</td>
<td></td>
</tr>
<tr>
<td>Input Frequency Range</td>
<td>50/60H</td>
<td>50/60H</td>
<td>50/60H</td>
<td>50/60H</td>
<td>50/60H</td>
<td>50/60H</td>
</tr>
<tr>
<td>Power @120VAC</td>
<td>5 W max</td>
<td>5 W max</td>
<td>6 W max</td>
<td>22 W max</td>
<td>26 W max</td>
<td>11 W max</td>
</tr>
<tr>
<td>Power @220 VAC</td>
<td>6 W max</td>
<td>6 W max</td>
<td>8 W max</td>
<td>28 W max</td>
<td>37 W max</td>
<td>17 W max</td>
</tr>
</tbody>
</table>
# Appendix B - Cabling, Hardware, & Electrical

## Table 25: Cyclades-TS environmental conditions

<table>
<thead>
<tr>
<th>Environmental Information</th>
<th>TS110/100</th>
<th>TS400</th>
<th>TS800</th>
<th>TS1000</th>
<th>TS2000</th>
<th>TS3000</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating Temperature</td>
<td>50°F to 122°F (10°C to 50°C)</td>
<td>50°F to 112°F (10°C to 44°C)</td>
<td>50°F to 112°F (10°C to 44°C)</td>
<td>50°F to 112°F (10°C to 44°C)</td>
<td>50°F to 112°F (10°C to 44°C)</td>
<td></td>
</tr>
<tr>
<td>Relative Humidity</td>
<td>10 - 90%, non-condensing</td>
<td>10 - 90%, non-condensing</td>
<td>10 - 90%, non-condensing</td>
<td>10 - 90%, non-condensing</td>
<td>10 - 90%, non-condensing</td>
<td></td>
</tr>
</tbody>
</table>

## Table 28: Cyclades-TS physical specifications

<table>
<thead>
<tr>
<th>Physical Information</th>
<th>TS100</th>
<th>TS110</th>
<th>TS400</th>
<th>TS800</th>
<th>TS1000</th>
<th>TS2000</th>
<th>TS3000</th>
</tr>
</thead>
<tbody>
<tr>
<td>External Dimensions</td>
<td>2.76 x 3.35 x 1.18 in.</td>
<td>3.4 x 4.8 x 1 in.</td>
<td>8.5 x 4.75 x 1 in.</td>
<td>8.5 x 4.75 x 1 in.</td>
<td>17 x 8.5 x 1.75 in.</td>
<td>17 x 8.5 x 1.75 in.</td>
<td></td>
</tr>
<tr>
<td>Weight</td>
<td>0.3 lb.</td>
<td>0.8 lb.</td>
<td>1.5 lb.</td>
<td>1.6 lb.</td>
<td>6 lb.</td>
<td>6.2 lb.</td>
<td>8 lb.</td>
</tr>
</tbody>
</table>

## Table 31: Cyclades-TS safety specifications

<table>
<thead>
<tr>
<th>Safety Information</th>
<th>TS110/100</th>
<th>TS400</th>
<th>TS800</th>
<th>TS1000</th>
<th>TS2000</th>
<th>TS3000</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approvals</td>
<td>FCC and CE, Class A</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Appendix B - Cabling, Hardware, & Electrical

The following section has all the information you need to quickly and successfully purchase or build cables to the Cyclades-TS. It focuses on information related to the RS-232 interface, which applies not only to the Cyclades-TS but also to any RS-232 cabling. At the end of this chapter you will also find some information about the RS-485 interface, which is available for the Cyclades-TS110/100 models only.

The RS-232 Standard

RS-232C, EIA RS-232, or simply RS-232 refer to a standard defined by the Electronic Industries Association in 1969 for serial communication. More than 30 years later, more applications have been found for this standard than its creators could have imagined. Almost all electronic devices nowadays have serial communication ports.

RS-232 was defined to connect Data Terminal Equipment, (DTE, usually a computer or terminal) to Data Communication Equipment (DCE, usually a modem):

DTE > RS-232 > DCE > communication line > DCE > RS-232 > DTE

RS-232 is now mostly being used to connect DTE devices directly (without modems or communication lines in between). While that was not the original intention, it is possible with some wiring tricks. The relevant signals (or wires) in a RS-232 cable, from the standpoint of the computer (DTE), are:

- **Receive Data (RxD) and Transmit Data (TxD)**
  - The actual data signals
- **Signal Ground (Gnd)**
  - Electrical reference for both ends
- **Data Terminal Ready (DTR)**
  - Indicates that the computer (DTE) is active
- **Data Set Ready (DSR)**
  - Indicates that the modem (DCE) is active.
- **Data Carrier Ready (DCD)**
  - Indicates that the connection over the communication line is active
- **CTS (Clear to Send, an input)**
  - Flow control for data flowing from DTE to DCE
- **RTS (Request to Send, an output)**
  - Flow control for data flowing from DCE to DTE
Appendix B - Cabling, Hardware, & Electrical

Not all signals are necessary for every application, so the RS-232 cable may not need all 7 wires. The RS-232 interface defines communication parameters such as parity, number of bits per character, number of stop-bits and the baud rate. Both sides must be configured with the same parameters. That is the first thing to verify if you think you have the correct cable and things still do not work. The most common configuration is 8N1 (8 bits of data per character, no parity bit included with the data, 1 stop-bit to indicate the end of a character). The baud rate in a RS-232 line translates directly into the data speed in bits per second (bps). Usual transmission speeds range between 9,600 bps and 19,200bps (used in most automation and console applications) to 115,200 bps (used by the fastest modems).

Cable Length

The original RS-232 specifications were defined to work at a maximum speed of 19,200 bps over distances up to 15 meters (or about 50 feet). That was 30 years ago. Today, RS-232 interfaces can drive signals faster and through longer cables.

As a general rule, consider:

- If the speed is lower than 38.4 kbps, you are safe with any cable up to 30 meters (100 feet)
- If the speed is 38.4 kbps or higher, cables should be shorter than 10 meters (30 feet)
- If your application is outside the above limits (high speed, long distances), you will need better quality (low impedance, low-capacitance) cables.

Successful RS-232 data transmission depends on many variables that are specific to each environment. The general rules above are empirical and have a lot of safety margins built-in.
Connectors

The connector traditionally used with RS-232 is the 25-pin D-shaped connector (DB-25). Most analog modems and most older computers and serial equipment use this connector. The RS-232 interface on DB-25 connector always uses the same standard pin assignment.

The 9-pin D-shaped connector (DB-9) saves some space and is also used for RS-232. Most new PC COM ports and serial equipment (specially when compact size is important) uses this connector. RS-232 interfaces on DB-9 connectors always use the same standard pin assignment.

The telephone-type modular RJ-45 plug and jack are very compact, inexpensive and compatible with the phone and Ethernet wiring systems present in most buildings and data centers. Most networking equipment and new servers use RJ-45 connectors for serial communication. Unfortunately there is no standard RS-232 pin assignment for RJ-45 connectors. Every equipment vendor has its own pin assignment.

Most connectors have two versions. The ones with pins are said to be “male” and the ones with holes are said to be “female.”

<table>
<thead>
<tr>
<th>RS-232 Signal</th>
<th>Name/Function (Input/Output)</th>
<th>DB-25 pins (Standard)</th>
<th>DB-9 pins (Standard)</th>
<th>RJ-45 pins (Cyclades)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chassis</td>
<td>Safety Ground</td>
<td>1</td>
<td>Shell</td>
<td>Shell</td>
</tr>
<tr>
<td>TxD</td>
<td>Transmit Data (O)</td>
<td>2</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>RxD</td>
<td>Receive Data (I)</td>
<td>3</td>
<td>2</td>
<td>6</td>
</tr>
<tr>
<td>DTR</td>
<td>Data Terminal Ready (O)</td>
<td>20</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>DSR</td>
<td>Data Set Ready (I)</td>
<td>6</td>
<td>6</td>
<td>8</td>
</tr>
<tr>
<td>DCD</td>
<td>Data Carrier Detect (I)</td>
<td>8</td>
<td>1</td>
<td>7</td>
</tr>
<tr>
<td>RTS</td>
<td>Request To Send (O)</td>
<td>4</td>
<td>7</td>
<td>1</td>
</tr>
<tr>
<td>CTS</td>
<td>Clear To Send (I)</td>
<td>5</td>
<td>8</td>
<td>5</td>
</tr>
<tr>
<td>Gnd</td>
<td>Signal Ground</td>
<td>7</td>
<td>5</td>
<td>4</td>
</tr>
</tbody>
</table>
Appendix B - Cabling, Hardware, & Electrical

**Straight-Through vs. Crossover Cables**

The RS-232 interface was originally intended to connect a DTE (computer, printer and other serial devices) to a DCE (modem) using a straight-through cable (all signals on one side connecting to the corresponding signals on the other side one-to-one). By using some “cabling tricks,” we can use RS-232 to connect two DTEs as is the case in most modern applications.

A crossover (a.k.a. null-modem) cable is used to connect two DTEs directly, without modems or communication lines in between. The data signals between the two sides are transmitted and received and there are many variations on how the other control signals are wired. A “complete” crossover cable would connect TxD with RxD, DTR with DCD/DSR, and RTS with CTS on both sides. A “simplified” crossover cable would cross TxD and RxD and locally short-circuit DTR with DCD/DSR and RTS with CTS.

**Which cable should be used?**

First, look up the proper cable for your application in the table below. Next, purchase standard off-the-shelf cables from a computer store or cable vendor. For custom cables, refer to the cable diagrams to build your own cables or order them from Cyclades or a cable vendor.

<table>
<thead>
<tr>
<th>To Connect To</th>
<th>Use Cable</th>
</tr>
</thead>
<tbody>
<tr>
<td>DCE DB-25 Female (standard)</td>
<td>Cable 1: RJ-45 to DB-25 M straight-through (Custom). This custom cable can be ordered from Cyclades or other cable vendors. A sample is included with the product (“straight-through”).</td>
</tr>
<tr>
<td>Analog Modems</td>
<td></td>
</tr>
<tr>
<td>ISDN Terminal Adapters</td>
<td></td>
</tr>
</tbody>
</table>
Table 33: Which cable to use

<table>
<thead>
<tr>
<th>To Connect To</th>
<th>Use Cable</th>
</tr>
</thead>
<tbody>
<tr>
<td>DTE RJ-45 Cyclades (custom)</td>
<td>Cable 2: RJ-45 to RJ-45 crossover (custom). A sample is included with the product (“straight-through”) This custom cable can be ordered from Cyclades or other cable vendors using the provided wiring diagram.</td>
</tr>
<tr>
<td>• All Cyclades Console Ports</td>
<td></td>
</tr>
<tr>
<td>DTE DB-25 to DB-9 Cyclades (custom)</td>
<td>Cable 3: DB-9 Female to DB-25 Female crossover. This connects the Cyclades-TS110/100 (serial port) to terminals, printers and other DTE RS-232 devices.</td>
</tr>
<tr>
<td>• For the Cyclades-TS110/100</td>
<td></td>
</tr>
</tbody>
</table>

Cable Diagrams

Before using the following cable diagrams refer to the tables above to select the correct cable for your application. Sometimes, crossover cables are wired slightly differently depending on the application. A “complete” crossover cable would connect the TxD with RxD, DTR with DCD/DSR, and RTS with CTS across both sides. A “simplified” crossover cable would cross TxD and RxD and locally short-circuit DTR with DCD/DSR and RTS with CTS.

Most of the diagrams in this document show the “complete” version of the crossover cables, with support for modem control signals and hardware flow control. Applications that do not require such features have just to configure NO hardware flow control and NO DCD detection on their side. Both ends should have the same configuration for better use of the complete version of the cables.

*These cables appear in Cable Package #1 and/or Cable Package #2. You may or may not find them in your box depending on which package you received.*
Appendix B - Cabling, Hardware, & Electrical

Cable #1: Cyclades RJ-45 to DB-25 Male, straight-through

Application: This cable connects Cyclades products (serial ports) to modems and other DCE RS-232 devices. It is included in both Cable Package #1 and #2.

![Cyclades RJ-45 to DB-25 Male, straight-through](image)

**Figure 37: Cable 1 - Cyclades RJ-45 to DB-25 Male, straight-through**

<table>
<thead>
<tr>
<th>RJ-45 Male</th>
<th>DB-25 Male</th>
</tr>
</thead>
<tbody>
<tr>
<td>TxD 3</td>
<td>TxD 2</td>
</tr>
<tr>
<td>RxD 6</td>
<td>RxD 3</td>
</tr>
<tr>
<td>Gnd 4</td>
<td>Gnd 7</td>
</tr>
<tr>
<td>DTR 2</td>
<td>DTR 20</td>
</tr>
<tr>
<td>DSR 8</td>
<td>DSR 6</td>
</tr>
<tr>
<td>DCD 7</td>
<td>DCD 8</td>
</tr>
<tr>
<td>RTS 1</td>
<td>RTS 4</td>
</tr>
<tr>
<td>CTS 5</td>
<td>CTS 5</td>
</tr>
</tbody>
</table>

Cable #2: Cyclades RJ-45 to DB-25 Female/Male, crossover

This cable connects Cyclades products (serial ports) to console ports, terminals, printers and other DTE RS-232 devices. If you are using Cable Package #1, after connecting the appropriate adapter to the RJ-45 straight-through cable, you will essentially have the cable shown in this picture. If you are using Cable Package #2, no assembly is required. You will have the cable shown below.

![Cyclades RJ-45 to DB-25 Female/Male, crossover](image)

**Figure 38: Cable 2 - Cyclades RJ-45 to DB-25 Female/Male, crossover**

<table>
<thead>
<tr>
<th>RJ-45 Custom</th>
<th>DB-25 F/M</th>
</tr>
</thead>
<tbody>
<tr>
<td>TxD 3</td>
<td>TxD 2</td>
</tr>
<tr>
<td>RxD 6</td>
<td>RxD 3</td>
</tr>
<tr>
<td>Gnd 4</td>
<td>Gnd 7</td>
</tr>
<tr>
<td>DTR 2</td>
<td>DTR 20</td>
</tr>
<tr>
<td>DSR 8</td>
<td>DSR 6</td>
</tr>
<tr>
<td>DCD 7</td>
<td>DCD 8</td>
</tr>
<tr>
<td>RTS 1</td>
<td>RTS 4</td>
</tr>
<tr>
<td>CTS 5</td>
<td>CTS 5</td>
</tr>
</tbody>
</table>
Appendix B - Cabling, Hardware, & Electrical

Cable #3: Cyclades RJ-45 to DB-9 Female, crossover

This cable connects Cyclades products (serial ports) to console ports, terminals, printers and other DTE RS-232 devices. If you are using Cable Package #1, after connecting the appropriate adapter to the RJ-45 straight-through cable, you will essentially have the cable shown in this picture. If you are using Cable Package #2, no assembly is required. You will have the cable shown below.

![Figure 39: Cable 3 - Cyclades RJ-45 to DB-9 Female, crossover](image)

Cable #4: Cyclades RJ-45 to Cyclades RJ-45, straight-through

This cable is the main cable that you will use. Along with one of the adapters provided (RJ-45 to DB-9 or RJ-45 to DB-25) you can create a crossover cable like the ones explained in Cable #2 or #3 for configuration or to connect to a server. This cable is only included in Cable Package #1.

![Figure 40: Cable 4 - Cyclades RJ-45 to Cyclades RJ-45, straight-through](image)
Appendix B - Cabling, Hardware, & Electrical

Cable #5: Cyclades/Sun Netra Cable

This Adapter attaches to a Cat 3 or Cat 5 network cable. It is usually used in console management applications to connect Cyclades products to a Sun Netra server or to a Cisco product. This cable is included in Cable Package #2.

![Cable 5 - Cyclades/Sun Netra Cable](image1)

<table>
<thead>
<tr>
<th>PLUG (Sun Netra/Cisco)</th>
<th>JACK (Cyclades)</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSR 8</td>
<td>RTS 1</td>
</tr>
<tr>
<td>DCD 7</td>
<td>DTR 2</td>
</tr>
<tr>
<td>RxD 6</td>
<td>TXD 3</td>
</tr>
<tr>
<td>GND 4</td>
<td>GND 4</td>
</tr>
<tr>
<td>CTS 5</td>
<td></td>
</tr>
<tr>
<td>RTS 1</td>
<td>CTS 5</td>
</tr>
<tr>
<td>TxD 3</td>
<td>RxD 6</td>
</tr>
<tr>
<td>DTR 2</td>
<td>DCD 7</td>
</tr>
</tbody>
</table>

*Figure 41: Cable 5 - Cyclades/Sun Netra Cable*

Adapters

The following four adapters are included in the product box. A general diagram is provided below and then a detailed description is included for each adapter.

Loop-Back Connector for Hardware Test

The use of the following DB-25 connector is explained in the Troubleshooting chapter. It is included in both Cable Package #1 and #2.

![Loop-Back Connector](image2)

*Figure 42: Loop-Back Connector*
Cyclades\Sun Netra Adapter

This Adapter attaches to a Cat 3 or Cat 5 network cable. It is usually used in console management applications to connect Cyclades products to a Sun Netra server or to a Cisco product. At one end of the adapter is the black CAT.5e Inline Coupler box with a female RJ-45 terminus, from which a 3-inch-long black Sun Netra-labeled cord extends, terminating in an RJ-45 male connector. This adapter is included in Cable Package #2.

<table>
<thead>
<tr>
<th>PLUG (Sun Netra/Cisco)</th>
<th>JACK (Cyclades)</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSR 8</td>
<td>RTS 1</td>
</tr>
<tr>
<td>DCD 7</td>
<td>DTR 2</td>
</tr>
<tr>
<td>RxD 6</td>
<td>TXD 3</td>
</tr>
<tr>
<td>GND 4</td>
<td>GND 4</td>
</tr>
<tr>
<td>CTS 5</td>
<td></td>
</tr>
<tr>
<td>RTS 1</td>
<td>CTS 5</td>
</tr>
<tr>
<td>TxD 3</td>
<td>RxD 6</td>
</tr>
<tr>
<td>DTR 2</td>
<td>DCD 7</td>
</tr>
</tbody>
</table>

Figure 43: Cyclades\Sun Netra Adapter

RJ-45 Female to DB-25 Male Adapter

The following adapter may be necessary. It is included in Cable Package #1.

<table>
<thead>
<tr>
<th>RJ-45</th>
<th>DB-25M</th>
</tr>
</thead>
<tbody>
<tr>
<td>RTS 1</td>
<td>5</td>
</tr>
<tr>
<td>DTR 2</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>8</td>
</tr>
<tr>
<td>TXD 3</td>
<td>3</td>
</tr>
<tr>
<td>GND 4</td>
<td>7</td>
</tr>
<tr>
<td>CTS 5</td>
<td>4</td>
</tr>
<tr>
<td>RxD 6</td>
<td>2</td>
</tr>
<tr>
<td>DCD 7</td>
<td></td>
</tr>
<tr>
<td>DSR 8</td>
<td></td>
</tr>
</tbody>
</table>

Figure 44: RJ-45 Female to DB-25 Male Adapter
Appendix B - Cabling, Hardware, & Electrical

RJ-45 Female to DB-25 Female Adapter

The following adapter may be necessary. It is included in Cable Package #1.

![Diagram of RJ-45 Female to DB-25 Female Adapter]

**Figure 45: RJ-45 Female to DB-25 Female Adapter**

RJ-45 Female to DB-9 Female Adapter

The following adapter may be necessary. This is included in Cable Package #1.

![Diagram of RJ-45 Female to DB-9 Female Adapter]

**Figure 46: RJ-45 Female to DB-9 Female Adapter**
The RS-485 Standard

The RS-485 is another standard for serial communication and is available only in the TS110/100. Different from the RS-232, the RS-485 uses fewer wires - either two wires (one twisted pair) for half duplex communication or four wires (two twisted pairs) for full duplex communication. Another RS-485 characteristic is the “termination.” In a network that uses the RS-485 standard, the equipment is connected one to the other in a cascade arrangement. A “termination” is required from the last equipment to set the end of this network.

TS110/100 Connectors

Although the RS-485 can be provided in different kinds of connectors, the Secure Console Port Server SSH 1-Port uses a 9-pin D-shaped connector (DB-9) and a Terminal Block with the pin assignment described below.

Table 35: TS110/100 Connector pin assignment

<table>
<thead>
<tr>
<th>RS-485 Signal</th>
<th>Name/Function</th>
<th>DB-9 pins</th>
<th>Terminal Block pins</th>
</tr>
</thead>
<tbody>
<tr>
<td>PW+</td>
<td>Not in use</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>TXD-</td>
<td>Transmit Data - (A)</td>
<td>7</td>
<td>2</td>
</tr>
<tr>
<td>TXD+</td>
<td>Transmit Data + (B)</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>RXD+</td>
<td>Receive Data + (B)</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>RXD-</td>
<td>Receive Data - (A)</td>
<td>8</td>
<td>5</td>
</tr>
<tr>
<td>PW-</td>
<td>Not in use</td>
<td></td>
<td>6</td>
</tr>
</tbody>
</table>
Appendix B - Cabling, Hardware, & Electrical

**TS110 Current Specifications**

Analog Ports - 100mA monetary  
10mA continuous  
90uA minimum

Digital Ports - Outputs - 10mA maximum  
3.6 mA minimum  
Inputs - 8.3 mA maximum  
3.6mA minimum

*Figure 47: Terminal Block Pins*

Notice that if the TS110/100 is configured to use RS-485, the RS-485 signals will be available in both DB-9 and Terminal Block. In this case, the DB-9 pins used in an RS-232 connection can be considered not connected.
Appendix B - Cabling, Hardware, & Electrical

**Cable Diagrams**

**Cable #1: DB-9 Female to DB-9 Female, crossover half duplex**

Application: It connects the TS110/100 (serial port) DTE RS-485 devices with half duplex communication.

![Cable Diagram 1](image)

*Figure 48: Cable 1 for the TS110/100 - DB-9 Female to DB-9 Female, crossover half duplex*

**Cable #2: DB-9 Female to DB-9 Female, crossover full duplex**

Application: It connects the TS110/100 (serial port) to DTE RS-485 devices with full duplex communication.

![Cable Diagram 2](image)

*Figure 49: Cable 2 for the TS110/100 - DB-9 Female to DB-9 Female, crossover full duplex*
Appendix B - Cabling, Hardware, & Electrical

Cable #3: Terminal Block to Terminal Block, crossover half duplex
Application: It connects the TS110/100 (serial port) to DTE RS-485 devices with half duplex communication.

<table>
<thead>
<tr>
<th>Terminal Block</th>
<th>Terminal Block</th>
</tr>
</thead>
<tbody>
<tr>
<td>RxD -5</td>
<td>RxD -5</td>
</tr>
<tr>
<td>TxD -2</td>
<td>TxD -2</td>
</tr>
<tr>
<td>RxD +4</td>
<td>RxD +4</td>
</tr>
<tr>
<td>TxD +3</td>
<td>TxD +3</td>
</tr>
</tbody>
</table>

*Figure 50: Cable 2 for the TS110/100 - Terminal Block to Terminal Block, crossover half duplex*

Cable #4: Terminal Block to Terminal Block, crossover full duplex
Application: It connects the TS110/100 (serial port) to DTE RS-485 devices with full duplex communication.

<table>
<thead>
<tr>
<th>Terminal Block</th>
<th>Terminal Block</th>
</tr>
</thead>
<tbody>
<tr>
<td>RxD -5</td>
<td>TxD -2</td>
</tr>
<tr>
<td>RxD +4</td>
<td>TxD +3</td>
</tr>
<tr>
<td>TxD -2</td>
<td>RxD -5</td>
</tr>
<tr>
<td>TxD +3</td>
<td>RxD +4</td>
</tr>
</tbody>
</table>

*Figure 51: Cable 4 for the TS110/100 - Terminal Block to Terminal Block, crossover full duplex*
Cable #5: DB-9 Female to DB-25 Female, crossover

This cable connects the TS110/100 to console ports, terminals, printers and other DTE RS-232 devices. You will essentially have the cable shown in this picture:

![Diagram of a crossover cable with DB-9 Female on the left and DB-25 Female on the right]

<table>
<thead>
<tr>
<th>Female DB9</th>
<th>Female DB25</th>
</tr>
</thead>
<tbody>
<tr>
<td>RxD 2</td>
<td>2 TxD</td>
</tr>
<tr>
<td>TxD 3</td>
<td>3 RxD</td>
</tr>
<tr>
<td>Gnd 5</td>
<td>7 Gnd</td>
</tr>
<tr>
<td>DSR 6</td>
<td>20 DTR</td>
</tr>
<tr>
<td>DCD 1</td>
<td></td>
</tr>
<tr>
<td>DTR 4</td>
<td>6 DSR</td>
</tr>
<tr>
<td></td>
<td>8 DCD</td>
</tr>
<tr>
<td>RTS 7</td>
<td>5 CTS</td>
</tr>
<tr>
<td>CTS 8</td>
<td>4 RTS</td>
</tr>
</tbody>
</table>

Figure 52: Cable 5 for the TS110/100 - DB-9 Female to DB-25 Female, crossover
Appendix C - The pslave Configuration File

Introduction

This chapter begins with a table containing parameters common to all profiles, followed by tables with parameters specific to a certain profile. You can find samples of the pslave configuration files (pslave.conf, .cas, .ts, and .ras) in the /etc/portslave directory in the TS box.

Configuration Parameters

CAS, TS, and Dial-in Common Parameters

The parameters on the following table are common to all three profiles:

Table 36: Parameters Common to CAS, TS, & Dial-in Access

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Value for this Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>conf.dhcp_client</td>
<td>It defines the dhcp client operation mode. Valid values: 0 - DHCP disabled</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>1 - DHCP active</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2 - DHCP active and the unit saves in flash the last IP assigned by the</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DHCP server (default).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Also see Description column.</td>
<td></td>
</tr>
<tr>
<td>conf.eth_ip_alias</td>
<td>Secondary IP address for the Ethernet interface (needed for clustering</td>
<td>209.81.55.10</td>
</tr>
<tr>
<td></td>
<td>feature).</td>
<td></td>
</tr>
<tr>
<td>conf.eth_mask_alias</td>
<td>Mask for the secondary IP address above.</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>conf.rlogin</td>
<td>It defines the location of rlogin utility</td>
<td>Ex: /bin/rlogin</td>
</tr>
<tr>
<td></td>
<td>Note: This is a parameter specific to TS profile.</td>
<td></td>
</tr>
<tr>
<td>conf.facility</td>
<td>The local facility sent to syslog-ng from PortSlave.</td>
<td>1 - 7</td>
</tr>
</tbody>
</table>
## Table 36: Parameters Common to CAS, TS, & Dial-in Access

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Value for this Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>conf.group</td>
<td>Used to group users to simplify the configuration of the parameter all.users later on. This parameter can be used to define more than one group.</td>
<td>group_name: user1, user2</td>
</tr>
<tr>
<td>conf.eth_ip</td>
<td>Configured in Task 4: Edit the pslave.conf file in Chapter 2 - Installation, Configuration, and Usage. This is the IP address of the Ethernet interface. This parameter, along with the next two, is used by the cy_ras program to OVERWRITE the file /etc/network/ifcfg_eth0 as soon as the command “signal_ras hup” is executed. The file /etc/network/ifcfg_eth0 should not be edited by the user unless the cy_ras configuration is not going to be used.</td>
<td>200.200.200.1</td>
</tr>
<tr>
<td>conf.eth_mask</td>
<td>The mask for the Ethernet network.</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>conf.eth_mtu</td>
<td>The Maximum Transmission Unit size, which determines whether or not packets should be broken up.</td>
<td>1500</td>
</tr>
<tr>
<td>conf.lockdir</td>
<td>The lock directory, which is /var/lock for the Cyclades-TS. It should not be changed unless the user decides to customize the operating system.</td>
<td>/var/lock</td>
</tr>
<tr>
<td>all.dcd</td>
<td>DCD signal (sets the tty parameter CLOCAL). Valid values are 0 or 1. If all.dcd=0, a connection request will be accepted regardless of the DCD signal and the connection will not be closed if the DCD signal is set to DOWN. If all.dcd=1 a connection request will be accepted only if the DCD signal is UP and the connection will be closed if the DCD signal is set to DOWN.</td>
<td>0</td>
</tr>
</tbody>
</table>
### Table 36: Parameters Common to CAS, TS, & Dial-in Access

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Value for this Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>all.users</td>
<td>Restricts access to ports by user name (only the users listed can access the port or, using the character “!” all but the users listed can access the port.) In this example, the users joe, mark and members of user_group cannot access the port. A single comma and spaces/tabs may be used between names. A comma may not appear between the “!” and the first user name. The users may be local, Radius or TacacsPlus. User groups (defined with the parameter conf.group) can be used in combination with user names in the parameter list. Notice that these are common users, not administrators.</td>
<td>! joe, mark, user_group</td>
</tr>
</tbody>
</table>
| all.issue   | This text determines the format of the login banner that is issued when a connection is made to the Cyclades-TS. \n represents a new line and \r represents a carriage return. Expansion characters can be used here. Value for this Example: \r\n\r
Welcome to terminal server %h port S%p \r\n\r
See Description column                                                                                                           |
| all.prompt  | This text defines the format of the login prompt. Expansion characters can be used here.                                      | %h login:                                                  |
## Appendix C - The pslave Configuration File

### Table 36: Parameters Common to CAS, TS, & Dial-in Access

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Value for this Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>all.media</td>
<td>It defines media type RS232/RS484 and operation mode half/full duplex.</td>
<td>See Description column</td>
</tr>
<tr>
<td></td>
<td><strong>Valid values for all products:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• rs232 - RS232 (default value). When configured sXX.flow is set to hard, only transmit if the CTS signal is asserted.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• rs232_half - RS232 with RTS legacy half duplex. Allows hardware flow control, when the parameter sXX.flow is set to hard. With hardware flow control, it asserts the RTS signal and only sends data when CTS is asserted. When sXX.flow is set to no the CTS signal is asserted while sending data.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• rs232_half_cts - RS232 with RTS legacy half duplex and CTS control. Configured along with sXX.flow no only sends (asserts RTS while sending), if the CTS signal is not asserted.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Valid values for the TS100/TS110 only:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• rs485_half - RS485 half duplex without terminator.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• rs485_half_terminator - RS485 half duplex with terminator.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• rs485_full_terminator - RS485 full duplex with terminator.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• rs422 - alike rs485_full_terminator.</td>
<td></td>
</tr>
<tr>
<td>all.netmask</td>
<td>It defines the network mask for the serial port.</td>
<td>255.255.255.255</td>
</tr>
<tr>
<td>all.mtu</td>
<td>It defines the maximum transmit unit</td>
<td>1500</td>
</tr>
<tr>
<td>all.mru</td>
<td>It defines the maximum receive unit</td>
<td>1500</td>
</tr>
</tbody>
</table>
### Appendix C - The pslave Configuration File

#### Table 36: Parameters Common to CAS, TS, & Dial-in Access

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Value for this Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>all.sysutmp</td>
<td>It defines whether portslave must write login records.</td>
<td>yes/no</td>
</tr>
<tr>
<td>all.syswtmp</td>
<td>It defines whether portslave must write login records.</td>
<td>yes/no</td>
</tr>
<tr>
<td>all.pmttype</td>
<td>Name of the IPDU manufacturer.</td>
<td>cyclades</td>
</tr>
<tr>
<td>all.pmusers</td>
<td>List of the outlets each user can access.</td>
<td>1-3</td>
</tr>
<tr>
<td>all.pmkey</td>
<td>The hotkey that identifies the power management command.</td>
<td>^p</td>
</tr>
<tr>
<td>all.pmNumOfOutlets</td>
<td>The number of outlets you have on the AlterPath PM.</td>
<td>8</td>
</tr>
<tr>
<td>sXX.pmsessions</td>
<td>Only users logged in with the connection method defined by this parameter will be allowed to access the IPDU unit. It is also necessary to define the authentication method in the sXX.authtype parameter and configure the sXX.users parameter in order to allow users to access the IPDU port. Valid values are: &quot;none&quot;, &quot;ssh&quot;, &quot;telnet&quot; or &quot;ssh_telnet&quot;.</td>
<td>ssh_telnet</td>
</tr>
</tbody>
</table>
## Appendix C - The pslave Configuration File

### Table 36: Parameters Common to CAS, TS, & Dial-in Access

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Value for this Example</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>all.sttyCmd</td>
<td>The TTY is programmed to work as configured and this user-specific configuration is applied over that serial port. Parameters must be separated by a space. The following example sets: -igncr, -onlcr, opost, -icrnl</td>
<td>commented</td>
<td>-igncr This tells the terminal not to ignore the carriage-return on input, -onlcr Do not map newline character to a carriage return or newline character sequence on output, opost Post-process output, -icrnl Do not map carriage-return to a newline character on input. all.sttyCmd -igncr -onlcr opost -icrnl</td>
</tr>
<tr>
<td>all.utmpfrom</td>
<td>It allow the administrator to customize the field &quot;FROM&quot; in the login records (utmp file). It is displayed in the &quot;w&quot; command.</td>
<td>See Description Column</td>
<td>Ex: &quot;$g:%P.%3.%4&quot; %g : process id %P : Protocol %3 : Third nibble of remote IP %J : Remote IP Note: In the pslave.conf file there is a list of all expansion variables available.</td>
</tr>
<tr>
<td>all.radnullpass</td>
<td>It defines whether the access to users with null password in the radius server must be granted or not.</td>
<td>yes/no</td>
<td></td>
</tr>
</tbody>
</table>
Table 36: Parameters Common to CAS, TS, & Dial-in Access

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Value for this Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>all.speed</td>
<td>The speed for all ports.</td>
<td>9600</td>
</tr>
<tr>
<td>all.datasize</td>
<td>The data size for all ports.</td>
<td>8</td>
</tr>
<tr>
<td>all.stopbits</td>
<td>The number of stop bits for all ports.</td>
<td>1</td>
</tr>
<tr>
<td>all.parity</td>
<td>The parity for all ports.</td>
<td>none</td>
</tr>
<tr>
<td>all.authhost1</td>
<td>This address indicates the location of the Radius/TacacsPlus authentication server and is only necessary if this option is chosen in the previous parameter. A second Radius/TacacsPlus authentication server can be configured with the parameter all.authhost2.</td>
<td>200.200.200.2</td>
</tr>
<tr>
<td>all.accthost1</td>
<td>This address indicates the location of the Radius/TacacsPlus accounting server, which can be used to track how long users are connected after being authorized by the authentication server. Its use is optional. If this parameter is not used, accounting will not be performed. If the same server is used for authentication and accounting, both parameters must be filled with the same address. A second Radius/TacacsPlus accounting server can be configured with the parameter all.accthost2.</td>
<td>200.200.200.2</td>
</tr>
</tbody>
</table>
## Appendix C - The pslave Configuration File

### Table 36: Parameters Common to CAS, TS, & Dial-in Access

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Value for this Example</th>
</tr>
</thead>
</table>
| all.authtype| Configured in [Task 4: Edit the pslave.conf file](#) in [Chapter 2 - Installation, Configuration, and Usage](#). Type of authentication used. There are several authentication type options:  
  - *none* (no authentication)  
  - *local* (authentication is performed using the /etc/passwd file)  
  - *remote* (This is for a terminal profile only. The unit takes in a username but does not use it for authentication. Instead it passes it to the remote server where it is then used for authentication.)  
  - *radius* (authentication is performed using a Radius authentication server)  
  - *TacacsPlus* (authentication is performed using a TacacsPlus authentication server)  
  - *ldap* (authentication is performed against an ldap database using an ldap server. The IP address and other details of the ldap server are defined in the file /etc/ldap.conf) | local                  |
### Table 36: Parameters Common to CAS, TS, & Dial-in Access

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Value for this Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>all.authtype (cont.)</td>
<td>• NIS - All authentication types but NIS follow the format all.authtype &lt;Authentication&gt;DownLocal or &lt;Authentication&gt; (e.g. all.authtype radius or radiusDownLocal or ldap or ldapDownLocal, etc). NIS requires all.authtype to be set as local, regardless if it will be &quot;nis&quot; or its &quot;Downlocal&quot; equivalent. The service related to &quot;nis&quot; or its &quot;Downlocal&quot; equivalent would be configured in the /etc/nsswitch.conf file, not in the /etc/portsage/pslave.conf file. Note that this parameter controls the authentication required by the Cyclades-TS. The authentication required by the device to which the user is connecting is controlled separately.</td>
<td></td>
</tr>
<tr>
<td>all.break_sequence</td>
<td>This parameter is the string that is used to send a break to the TTY. It is only valid if TTY protocol is socket_ssh or socket_server.</td>
<td>~break</td>
</tr>
</tbody>
</table>
### Table 36: Parameters Common to CAS, TS, & Dial-in Access

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Value for this Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>all.break_interval</td>
<td>This parameter defines the break duration in milliseconds. It is valid if TTY protocol is socket_ssh,socket_server or ssh-2 (client).</td>
<td></td>
</tr>
<tr>
<td>all.radtimeout</td>
<td>This is the timeout (in seconds) for a Radius/TacacsPlus authentication query to be answered. The first server (authhost1) is tried “radretries” times, and then the second (authhost2), if configured, is contacted “radretries” times. If the second also fails to respond, Radius/TacacsPlus authentication fails.</td>
<td>3</td>
</tr>
<tr>
<td>all.radretries</td>
<td>Defines the number of times each Radius/TacacsPlus server is tried before another is contacted. The default, if not configured, is 5.</td>
<td>5</td>
</tr>
<tr>
<td>all.secret</td>
<td>This is the shared secret necessary for communication between the Cyclades-TS and the Radius/TacacsPlus servers.</td>
<td>secret</td>
</tr>
<tr>
<td>all.flow</td>
<td>This sets the flow control to hardware, software, or none. Valid values are: hard, none and soft.</td>
<td>hard</td>
</tr>
<tr>
<td>all.protocol</td>
<td>The default CAS setup was explained in Chapter 2, Task 4: Edit the pslave.conf file. The TS configuration settings are in Table 38, “TS Parameters,” on page 383. The Dial-in configuration settings are in Table 39, “Dial-in configuration Parameters,” on page 384.</td>
<td>socket_server</td>
</tr>
<tr>
<td>all.web_WinEMS</td>
<td>Defines whether or not management of Windows Emergency Management Service is allowed from the Web.</td>
<td>yes or 1, or no or 0</td>
</tr>
</tbody>
</table>
### Table 36: Parameters Common to CAS, TS, & Dial-in Access

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Value for this Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>all.xml_monitor</td>
<td>A non-zero value activates XML monitoring. All XML data received from the port is captured and sent to syslog-ng with facility LOCAL&lt;DB_facility&gt; and priority INFO. The format of the message is &quot;XML_MONITOR (ttySx) [data]&quot;. XML tags are sent by Windows Server 2003 Emergency Management Services during boot or crash. You can read more on XML_MONITOR in: /etc/syslog-ng/syslog-ng.conf</td>
<td>1</td>
</tr>
<tr>
<td>all.translation</td>
<td>Defines whether or not to perform translation of Fn-keys (e.g. F8 key) from one terminal type to VT-UTF8. Currently only translation from xterm to VT-UTF8 is supported.</td>
<td>xterm</td>
</tr>
<tr>
<td>sX.pmoutlet</td>
<td>sX indicates the serial port number to which the PM hardware is connected. The pmoutlet part of the parameter indicates the outlet # on the PM hardware that manages the server/network equipment in question.</td>
<td>8</td>
</tr>
<tr>
<td>s1.tty</td>
<td>The device name for the port is set to the value given in this parameter. If a device name is not provided for a port, it will not function.</td>
<td>ttyS1</td>
</tr>
</tbody>
</table>
Appendix C - The pslave Configuration File

CAS Parameters

You can configure additional CAS features with the parameters given on the following tables. (The is used as an example in some parameters.

In addition to the above parameters which are common to all local and remote access scenarios, you can also configure the following parameters for additional options. Many of the parameters are unique to CAS, but some also apply to TS and Dial-in port profiles. This is indicated in these instances.

Table 37: Mostly CAS-specific Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Value for this Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>conf.nfs_data_buffering</td>
<td>This is the Remote Network File System where data captured from the serial port will be written instead of being written to the local directory /var/run/DB. The directory tree to which the file will be written must be NFS-mounted, so the remote host must have NFS installed and the administrator must create, export and allow reading/writing to this directory. The size of this file is not limited by the value of the parameter all.data_buffering, though the value cannot be zero since a zero value turns off data buffering. The size of the file is dependent on the NFS server only (hard drive, partition size, etc.).</td>
<td>commented</td>
</tr>
<tr>
<td>conf.DB_facility</td>
<td>This value (0-7) is the Local facility sent to the syslog with the data when syslog_buffering is active. The file /etc/syslog-ng/syslog-ng.conf contains a mapping between the facility number and the action.</td>
<td>0</td>
</tr>
</tbody>
</table>
## Appendix C - The pslave Configuration File

### Table 37: Mostly CAS-specific Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Value for this Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>all.ipno</td>
<td>This is the default IP address of the Cyclades-TS 's serial ports. The “+” indicates that the first port should be addressed as 192.168.1.101 and the following ports should have consecutive values. Any host can access a port using its IP address as long as a path to the address exists in the host's routing table.</td>
<td>192.168.170.1 01+</td>
</tr>
<tr>
<td>all.netmask</td>
<td>It defines the network mask for the serial port.</td>
<td>255.255.255.2 55</td>
</tr>
<tr>
<td>all.DTR_reset</td>
<td>This parameter specifies the behavior of the DTR signal in the serial port. If set to zero the DTR signal will be ON if there is a connection to the serial port, otherwise OFF. If set from 1 to 99 the DTR signal will be always ON. A value greater or equal 100 specifies for how long (in milliseconds) the DTR signal will be turned off before it is turned back on again when a connection to the serial port is closed.</td>
<td>100</td>
</tr>
<tr>
<td>all.break_sequence</td>
<td>This parameter is the string that is used to send a break to the TTY. It is only valid if TTY protocol is socket_ssh or socket_server.</td>
<td>~break</td>
</tr>
<tr>
<td>all.break_interval</td>
<td>This parameter defines the break duration in miliseconds. It is valid if TTY protocol is socket_ssh,</td>
<td>socket_server or ssh-2 (client)</td>
</tr>
<tr>
<td>all.modbus_smode</td>
<td>Communication mode through the serial ports. This parameter is meaningful only when modbus protocol is configured. The valid options are ascii (normal TX/RX mode) and rtu (some time constraints are observed between characters while transmitting a frame). If not configured, ASCII mode will be assumed.</td>
<td>commented</td>
</tr>
</tbody>
</table>
### Appendix C - The pslave Configuration File

#### Table 37: Mostly CAS-specific Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Value for this Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>all.lf_suppress</td>
<td>This can be useful because telneting (from DOS) from some OS such as Windows 98 causes produces an extra line feed so two prompts appear whenever you press Enter. When set to 1, line feed suppression is active which will eliminate the extra prompt. When set to 0 (default), line feed suppression is not active.</td>
<td>0</td>
</tr>
<tr>
<td>all.auto_answer_input</td>
<td>This parameter works in conjunction with all.auto_answer_output. It allows you to configure a string that will be matched against all data coming in from the tty (remote server). If there is a match, the configured output string (auto_answer_output) will then be send back to the tty. This parameter works only when there is no session to the port. If uncommented and a string of bytes is set, matching occurs whenever there is not session established to the port. If this parameter is commented out, then no checking and matching occurs.</td>
<td>commented</td>
</tr>
</tbody>
</table>
Table 37: Mostly CAS-specific Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Value for this Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>all.auto_answer_output</td>
<td>This parameter works in conjunction with all.auto_answer_input. It allows you to configure a string that is sent back to the remote server whenever the incoming data remote server matches with all.auto_answer_input. This parameter works only when there is no session to the port. If this parameter is commented, then nothing will be sent back to the remote server even if all.auto_answer_input is uncommented. If this parameter is uncommented and if all.auto_answer_input is also uncommented, then the string configured will be sent back to the remote server.</td>
<td>commented</td>
</tr>
<tr>
<td>all.poll_interval</td>
<td>Valid only for protocols socket_server and raw_data. When not set to zero, this parameter sets the wait for a TCP connection keep-alive timer. If no traffic passes through the Cyclades-TS for this period of time, the Cyclades-TS will send a line status message to the remote device to see if the connection is still up. If not configured, 1000 ms is assumed (the unit for this parameter is ms). If set to zero, line status messages will not be sent to the socket client.</td>
<td>0</td>
</tr>
</tbody>
</table>
### Appendix C - The pslave Configuration File

#### Table 37: Mostly CAS-specific Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Value for this Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>all.socket_port</td>
<td>In the CAS profile, this defines an alternative labeling system for the Cyclades-TS ports. The “+” after the numerical value causes the serial interfaces to be numbered consecutively. In this example, serial interface 1 is assigned the port value 7001, serial interface 2 is assigned the port value 7002, etc. One example on how this could be used is in the case of all.protocol or s&lt;n&gt;.protocol socket_ssh and the port value (7001, 7002, etc), if supplied by the ssh client like username:port value, the ssh client will be directly connected with the serial interface. For TS, this parameter is valid only all.protocol is configured as socket_cliente or telnet. It is the TCP port number of the application that will accept connection requested by this serial port.</td>
<td>7001+</td>
</tr>
</tbody>
</table>
Appendix C - The pslave Configuration File

Table 37: Mostly CAS-specific Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Value for this Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>all.data_buffering</td>
<td>A non zero value activates data buffering (local or remote, according to what was configured in the parameter conf.nfs_data_buffering). If local data buffering, a file is created on the Cyclades-TS; if remote, a file is created through NFS in a remote server. All data received from the port is captured in this file. If local data buffering, this parameter means the maximum file size (in bytes). If remote, this parameter is just a flag to activate (greater than zero) or deactivate data buffering. When local data buffering is used, each time the maximum is reached the oldest 10% of stored data is discarded, releasing space for new data (FIFO system) - circular file. When remote data buffering is used, there's no maximum file size other than the one imposed by the remote server - linear file. This file can be viewed using the normal Unix tools (cat, vi, more, etc.). Size is in bytes not kilobytes. See Data Buffering for details.</td>
<td>0</td>
</tr>
</tbody>
</table>
Appendix C - The pslave Configuration File

Table 37: Mostly CAS-specific Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Value for this Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>all.DB_mode</td>
<td>When configured as cir for circular format, the buffer works like a revolving file at all times. The file is overwritten whenever the limit of the buffer size (as configured in all.data_buffering or s&lt;n&gt;.data_buffering) is reached. As for linear format (lin), once the limit of the kernel buffer size is reached (4k), a flow control stop (RTS off or XOFF-depending on how all.flow or s&lt;n&gt;.flow is set) is issued automatically to the remote device so that it will stop sending data to the serial port. Then, when a session is established to the serial port, the data in the buffer is shown to the user if not empty (don't_show_DBmenu parameter assumed to be 2), cleared, and a flow control start (RTS on or XON) is issued to resume data transmission. Once exiting the session, linear data buffering resumes. If all.flow or s&lt;n&gt;.flow is set to none, linear buffering is not possible as there is no way to stop reception through the serial line. Default is cir.</td>
<td>cir</td>
</tr>
<tr>
<td>all.DB_timestamp</td>
<td>Records the time stamp in the data buffering file (1) or not (0). If it is configured as 1, the software will accumulate input characters until it receives a CR and LF from the serial port or the accumulated data reaches 256 characters. Either way, the accumulated data will be recorded in the data buffering file along with the current time. The parameter all.data_buffering has to be with a non-zero value for this parameter to be meaningful.</td>
<td>0</td>
</tr>
</tbody>
</table>
### Table 37: Mostly CAS-specific Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Value for this Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>all.syslog_buffering</td>
<td>When non zero, the contents of the data buffer are sent to the syslogng every time a quantity of data equal to this parameter is collected. The syslog level for data buffering is hard coded to level 5 (notice) and facility local[0+conf.DB_facility]. The file /etc/syslog-ng/syslog-ng.conf should be set accordingly for the syslog-ng to take some action. <em>(See <a href="#">Syslog-ng Configuration to use with Syslog Buffering Feature</a>).</em></td>
<td>0</td>
</tr>
<tr>
<td>all.syslog_sess</td>
<td>Syslog_buffering must be activated for the following to work. When 0, syslog messages are always generated whether or not there is a session to the port sending data to the unit. When 1, syslog messages are NOT generated when there IS a session to the port sending data to the unit, but resumes generation of syslog messages when there ISN’T a session to the port.</td>
<td>0</td>
</tr>
<tr>
<td>all.dont_show_DBmenu</td>
<td>When zero, a menu with data buffering options is shown when a nonempty data buffering file is found. When 1, the data buffering menu is not shown. When 2, the data buffering menu is not shown but the data buffering file is shown if not empty. When 3, the data buffering menu is shown, but without the erase and show and erase options.</td>
<td>1</td>
</tr>
</tbody>
</table>
## Table 37: Mostly CAS-specific Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Value for this Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>all.alarm</td>
<td>When non zero, all data received from the port are captured and sent to syslog-ng with level INFO and local[0+conf.DB_facility]facility. The syslogng.conf file should be set accordingly, for the syslog-ng to take some action (please see Generating Alarms in Chapter 3 - Additional Features for the syslog-ng configuration file).</td>
<td>0</td>
</tr>
<tr>
<td>all.billing_records</td>
<td>Billing file size configuration. A non-zero value defines the maximum number of billing records within a billing file. Zero stops billing recording. The billing files are located at /var/run/DB and are named cycXXXXX-YYMMDD.hhmmss.txt (e.g., cycTS100-030122.153611.txt).</td>
<td>50</td>
</tr>
<tr>
<td>all.billing_timeout</td>
<td>Billing timeout configuration. A non-zero value defines how long (minutes) a billing file should be waiting for records before close. After a file is closed, this file is available for transfer and a new one is opened. Zero means “no timeout” and so the file is only closed after “billing_records” are received.</td>
<td>60</td>
</tr>
<tr>
<td>all.billing_eor</td>
<td>Defines the character sequence that terminates each billing record. Any character sequence is valid, including \r or ^M (carriage return), \n or ^J (new line), etc...”</td>
<td>Default value: &quot;\n&quot;</td>
</tr>
</tbody>
</table>
## Appendix C - The pslave Configuration File

### Table 37: Mostly CAS-specific Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Value for this Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>all.sniff_mode</td>
<td>This parameter determines what other users connected to the very same port (see parameter admin_users below) can see of the session of the first connected user (main session): in shows data written to the port, out shows data received from the port, and i/o shows both streams, whereas no means sniffing is not permitted. The second and later sessions are called sniff sessions and this feature is activated whenever the protocol parameter is set to socket_ssh or socket_server.</td>
<td>out</td>
</tr>
<tr>
<td>all.admin_users</td>
<td>This parameter determines which users can receive the sniff session menu. Then they have options to open a sniff session or cancel a previous session. When users want access per port to be controlled by administrators, this parameter is obligatory and authtype must not be none. User groups (defined with the parameter conf.group) can be used in combination with user names in the parameter list.</td>
<td>peter, john, user_group</td>
</tr>
<tr>
<td>all.multiple_sessions</td>
<td>Allows users to open more than one common and sniff session on the same port. The options are “yes,” “no,” “RW_session,” or “sniff_session.” Default is set to “no.”</td>
<td>no</td>
</tr>
<tr>
<td>all.escape_char</td>
<td>This parameter determines which character must be typed to make the session enter “menu mode”. The possible values are &lt;CTRL-a&gt; to &lt;CTRL-z&gt;. Represent the CTRL with ‘^’. This parameter is only valid when the port protocol is socket_server or socket_ssh. Default value is ‘^z’.</td>
<td>^z</td>
</tr>
</tbody>
</table>
## Appendix C - The pslave Configuration File

### Table 37: Mostly CAS-specific Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Value for this Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>all.tx_interval</td>
<td>Valid for protocols socket_server and raw_data. Defines the delay (in milliseconds) before transmission to the Ethernet of data received through a serial port. If not configured, 100ms is assumed. If set to zero or a value above 1000, no buffering will take place.</td>
<td>100</td>
</tr>
<tr>
<td>all.idletimeout</td>
<td>Specifies how long (in minutes) a connection can remain inactive before it is cut off. If it set to zero, the connection will not time out.</td>
<td>0</td>
</tr>
<tr>
<td>s1.serverfarm</td>
<td>Alias name given to the server connected to the serial port. Server_connected.</td>
<td>serial1</td>
</tr>
<tr>
<td>s2.tty</td>
<td>It defines the physical device name associated to the serial port (without the /dev/).</td>
<td>ttyS2</td>
</tr>
<tr>
<td>s8.tty</td>
<td>It defines the physical device name associated to the serial port (without the /dev/).</td>
<td>ttyS8</td>
</tr>
</tbody>
</table>
### TS Parameters

The following parameters are unique to a TS setup except where indicated.

Table 38: TS Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Value for this Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>conf.telnet</td>
<td>Location of the telnet utility</td>
<td>/usr/bin/telnet</td>
</tr>
<tr>
<td>conf.ssh</td>
<td>Location of the ssh utility.</td>
<td>/bin/ssh</td>
</tr>
<tr>
<td>conf.locallogins</td>
<td>This parameter is only necessary when authentication is being performed for a port. When set to one, it is possible to log in to the Cyclades-TS directly by placing a “!” before your login name, then using your normal password. This is useful if the Radius authentication server is down.</td>
<td>0</td>
</tr>
<tr>
<td>all.host</td>
<td>The IP address of the host to which the terminals will connect.</td>
<td>200.200.200.3</td>
</tr>
<tr>
<td>all.term</td>
<td>This parameter defines the terminal type assumed when performing rlogin or telnet to other hosts.</td>
<td>vt100</td>
</tr>
<tr>
<td>all.userauto</td>
<td>Username used when connected to a UNIX server from the user's serial terminal.</td>
<td></td>
</tr>
<tr>
<td>all.protocol (for TS)</td>
<td>For the terminal server configuration, the possible protocols are login (which requests username and password), rlogin (receives username from the TS and requests a password), telnet, ssh, ssh2, or socket_client. See all.socket_port definition if all.protocol is configured as socket_client.</td>
<td>rlogin</td>
</tr>
<tr>
<td>all.socket_port</td>
<td>The socket_port is the TCP port number of the application that will accept connection requested by this serial port. That application usually is telnet (23).</td>
<td></td>
</tr>
</tbody>
</table>
Appendix C - The pslave Configuration File

Table 38: TS Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Value for this Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>all.telnet_client_mode</td>
<td>When the protocol is TELNET, this parameter configured as BINARY (1) causes an attempt to negotiate the TELNET BINARY option on both input and output with the Telnet server. So it puts the telnet client in binary mode. The acceptable values are &quot;0&quot; or &quot;1&quot;, where &quot;0&quot; is text mode (default) and &quot;1&quot; is a binary mode.</td>
<td></td>
</tr>
<tr>
<td>s16.tty (TS)</td>
<td>It defines the physical device name associated to the serial port (without the /dev/).</td>
<td>ttyS16</td>
</tr>
</tbody>
</table>

Dial-in Access Parameters

The following parameters are unique to a Dial-in setup except where indicated.

Table 39: Dial-in configuration Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Value for this Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>conf.pppd</td>
<td>Location of the ppp daemon with Radius.</td>
<td>/usr/local/sbin/pppd</td>
</tr>
<tr>
<td>all.netmask</td>
<td>It defines the network mask for the serial port.</td>
<td>255.255.255.255</td>
</tr>
<tr>
<td>all.ipno (CAS and Dial-in)</td>
<td>See description in CAS section.</td>
<td></td>
</tr>
</tbody>
</table>
### Appendix C - The pslave Configuration File

#### Table 39: Dial-in configuration Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Value for this Example</th>
</tr>
</thead>
</table>
| all.initchat  | Modem initialization string.                                                | TIMEOUT 10 
\d\dATZ \nOK\r\n-ATZ-OK\r\n "" \n "" ATMO OK\r\n "" \n TIMEOUT 3600 RING "" \n STATUS Incoming %p:I.HANDSHAKE "" ATA\n TIME OUT 60 CONNECT@ "" \n STATUS Connected %p:I.HANDSHAKE |
| all.autoppp   | all.autoppp PPP options to auto-detect a ppp session. The cb-script parameter defines the file used for callback and enables negotiation with the callback server. Callback is available in combination with Radius Server authentication. When a registered user calls the TS, it will disconnect the user, then call the user back. The following three parameters must be configured in the Radius Server: attribute Service_type(6): Callback Framed; attribute Framed_Protocol(7): PPP; attribute Callback_Number(19): the dial number (example: 50903300). | %i:%j novj \proxyarp modem asyncmap 000A0000 \noipx noccp login auth require-pap refuse-chap\mtu %t mr u %t \cb-script /etc/portslave/cb_script \plugin /usr/lib/libpsr.so |
Appendix C - The pslave Configuration File

Table 39: Dial-in configuration Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Value for this Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>all.pppopt</td>
<td>all.pppopt PPP options when user has already been authenticated.</td>
<td>%i:%j novj \ proxyarp modem asyncmap 000A0000 \ noipx noccp mtu %t mru %t netmask%m \ idle %I maxconnect %T \ plugin /usr/lib/libpsr.so</td>
</tr>
<tr>
<td>all.protocol</td>
<td>For the Dial-in configuration, the available protocols are ppp, ppp_only, slip, and cslip.</td>
<td>ppp</td>
</tr>
<tr>
<td>s32.tty</td>
<td>See the s1.tty entry in the CAS section.</td>
<td>ttyS32</td>
</tr>
</tbody>
</table>
Appendix D - Upgrades and Troubleshooting

Upgrades

Users should upgrade the Cyclades-TS whenever there is a bug fix or new features that they would like to have. Below are the six files added by Cyclades to the standard Linux files in the /proc/flash directory when an upgrade is needed. They are:

- boot_ori - original boot code
- boot_alt - alternate boot code
- syslog - event logs (not used by Linux)
- config - configuration parameters, only the boot parameters are used by the boot code
- zImage - Linux kernel image
- script - file where all Cyclades-TS configuration information is stored

The Upgrade Process

To upgrade the Cyclades-TS, follow these steps:

**Step 1:** Log in to the TS as root.

Provide the root password if requested.

**Step 2:** Go to the /proc/flash directory using the following command:

```
cd /proc/flash
```

**Step 3:** FTP to the host where the new firmware is located.

Log in using your username and password. Go to the directory where the firmware is located. Select binary transfer and “get” the firmware file.

**Note:** The destination file name in the /proc/flash directory must be zImage. Example (hostname = server; directory = /tftpboot; username= admin; password = adminpw; firmware filename on that server = zImage.134).
Appendix D - Upgrades and Troubleshooting

ftp
> open server
> user admin
> Password: adminpw
> cd /tftpboot
> bin
> get zImage.134 zImage
> quit

Note: Due to space limitations, the new zImage file may not be downloaded with a different name, then renamed. The TS searches for a file named zImage when booting and there is no room in flash for two zImage files.

Step 4: Run zImage.
To make sure the downloaded file is not corrupted or that the zImage saved in flash is OK the user should run:

```
md5sum -b /proc/flash/zImage
```

Step 5: Check text file information.
Now the user should check with the information present in the text file saved in the Cyclades site (e.g. zImage.134.md5sum). If the numbers match, the downloaded file is not corrupted.

Step 6: Issue the command reboot.

```
reboot
```

Step 7: Confirm that the new Linux kernel has taken over.
After rebooting, the new Linux kernel will take over. This can be confirmed by typing the following to see the Linux kernel version:

```
cat /proc/version
```
Appendix D - Upgrades and Troubleshooting

Troubleshooting

Flash Memory Loss
If the contents of flash memory are lost after an upgrade, please follow the instructions below to restore your system:

Step 1: Turn the TS OFF, then back ON.

Step 2: Using the console, wait for the self test messages.
   If you haven’t got any, make sure you have the right settings. If you really get no boot message, press <s> right after powering ON and skip ALTERNATE boot code. That will make the boot run its ORIGINAL boot code.

Step 3: During the self test, press <Esc> after the Ethernet test.

Step 4: When the Watch Dog Timer prompt appears, press <Enter>.

Step 5: Choose the option Network Boot when asked.

Step 6: Enter the IP address of the Ethernet interface.

Step 7: Enter the IP address of the host where the new zImage file is located.

Step 8: Enter the file name of the zImage file on the host.

Step 9: Select the TFTP option instead of BOOTP.
   The host must be running TFTP and the new zImage file must be located in the proper directory. e.g. /tftpboot for Linux.

Step 10: Accept the default MAC address by pressing <Enter>.
   The Cyclades-TS should begin to boot off the network and the new image will be downloaded and begin running in RAM. At this point, follow the upgrade steps above (login, cd /proc/flash, ftp, and so forth) to save the new zImage file into flash again.
If the Cyclades-TS booted properly, the interfaces can be verified using `ifconfig` and `ping`. If ping does not work, check the routing table using the command `route`. Of course, all this should be tried after checking that the cables are connected correctly.

The file `/etc/config_files` contains a list of files acted upon by `saveconf` and `restoreconf`. If a file is missing, it will not be loaded onto the ramdisk on boot. The following table lists files that should be included in the `/etc/config_files` file and which programs use each.

<table>
<thead>
<tr>
<th>File</th>
<th>Program</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>/etc/securetty</code></td>
<td>telnet, login, su</td>
</tr>
<tr>
<td><code>/etc/issue</code></td>
<td>getty</td>
</tr>
<tr>
<td><code>/etc/getty_ttyS0</code></td>
<td>login (via console)</td>
</tr>
<tr>
<td><code>/etc/hostname</code></td>
<td>tcp</td>
</tr>
<tr>
<td><code>/etc/hosts</code></td>
<td>tcp</td>
</tr>
<tr>
<td><code>/etc/host.conf</code></td>
<td>tcp</td>
</tr>
<tr>
<td><code>/etc/nsswitch.conf</code></td>
<td>dns</td>
</tr>
<tr>
<td><code>/etc/resolv.conf</code></td>
<td>dns</td>
</tr>
<tr>
<td><code>/etc/config_files</code></td>
<td>saveconf</td>
</tr>
<tr>
<td><code>/etc/passwd</code></td>
<td>login, passwd, adduser...</td>
</tr>
<tr>
<td><code>/etc/group</code></td>
<td>login, passwd, adduser...</td>
</tr>
</tbody>
</table>
## Appendix D - Upgrades and Troubleshooting

**Table 40: Files to be included in `/etc/config_file` and the program to use**

<table>
<thead>
<tr>
<th>File</th>
<th>Program</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>/etc/ssh/ssh_host_key.pub</code></td>
<td>sshd</td>
</tr>
<tr>
<td><code>/etc/ssh/sshd_config</code></td>
<td>sshd</td>
</tr>
<tr>
<td><code>/etc/ssh/ssh_config</code></td>
<td>ssh client</td>
</tr>
<tr>
<td><code>/etc/ssh/ssh_host_key</code></td>
<td>sshd (ssh1)</td>
</tr>
<tr>
<td><code>/etc/ssh/ssh_host_key.pub</code></td>
<td>sshd (ssh1)</td>
</tr>
<tr>
<td><code>/etc/ssh/ssh_host_dsa_key</code></td>
<td>sshd (ssh2)</td>
</tr>
<tr>
<td><code>/etc/ssh/ssh_host_dsa_key.pub</code></td>
<td>sshd (ssh2)</td>
</tr>
<tr>
<td><code>/etc/snmp/snmpd.conf</code></td>
<td>snmpd</td>
</tr>
<tr>
<td><code>/etc/portsave/pslave.conf</code></td>
<td>cy_ras, portslave,TS configuration information</td>
</tr>
<tr>
<td><code>/etc/network/ifcfg_eth0</code></td>
<td>ifconfig eth0, cy_ras, rc.sysinit</td>
</tr>
<tr>
<td><code>/etc/network/ifcfg*</code></td>
<td>ifconfig, cy_ras, rc.sysinit</td>
</tr>
<tr>
<td><code>/etc/network/ifcfg_lo ifconfig</code></td>
<td>lo, cy_ras, rc.sysinit</td>
</tr>
<tr>
<td><code>/var/run/radsession.id</code></td>
<td>radinit, radius authentication process</td>
</tr>
<tr>
<td><code>/home</code></td>
<td>adduser, passwd</td>
</tr>
<tr>
<td><code>/etc/network/st_routes</code></td>
<td>ifconfig, cy_ras, rc.sysinit</td>
</tr>
<tr>
<td><code>/etc/syslog-ng/syslog-ng.conf</code></td>
<td>syslog-ng</td>
</tr>
</tbody>
</table>

**Important!** If any of the files listed in `/etc/config_files` is modified, the Cyclades-TS administrator must execute the command `saveconf` before rebooting the Cyclades-TS or the changes will be lost. If a file is created (or a filename altered), its name must be added to this file before executing `saveconf` and rebooting.
Appendix D - Upgrades and Troubleshooting

Important! Cyclades Technical Support is always ready to help with any configuration problems. Before calling, execute the command

cat /proc/version

and note the Linux version and Cyclades-TS version written to the screen. This will speed the resolution of most problems.

Hardware Test

A hardware test called tstest is included with the Cyclades-TS firmware. It is a menu-driven program, run by typing tstest at the command prompt. The various options are described below. Note that the Cyclades-TS should not be tested while in use as the test will inactivate all ports. You should inactivate all processes that may use the serial ports: inetd, sshd, cy_ras, and cy_buffering. Following are the hardware test steps:

Step 1: signal_ras stop.

Step 2: Perform all hardware tests needed.

Step 3: signal_ras start.

Port Test

Either a cross cable or a loop-back connector is necessary for this test. Their pinout diagrams are supplied in Appendix B - Cabling, Hardware, and Electrical Specifications. Connect the loop-back connector to the modem cable and then connect the modem cable to the port to be tested (or connect a cross cable between two ports to be tested). In the case of the 1-PortTS110/100, connect the DB-25 loop-back connector to the console cable using a DB-9 - DB-25 convertor. When tstest senses the presence of the cable or connector, the test will be run automatically and the result shown on the screen.

Each line of data corresponds to a port in test. The last four columns (DATA, CTS, DCD, and DSR) indicate errors. The values in these columns should be zero. Below is an example of the output screen.
Appendix D - Upgrades and Troubleshooting

<table>
<thead>
<tr>
<th>&lt;- Packets -&gt;</th>
<th>&lt;- Errors -&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>From</td>
<td>To</td>
</tr>
<tr>
<td>2 &lt;-&gt; 2</td>
<td>35</td>
</tr>
<tr>
<td>4 &lt;-&gt; 5</td>
<td>35</td>
</tr>
<tr>
<td>5 &lt;-&gt; 4</td>
<td>35</td>
</tr>
</tbody>
</table>

When this test is run with a cable or connector without the DSR signal (see the pinout diagram for the cable or connector being used), errors will appear in the DSR column. This does not indicate a problem with the port. In the example above, tsTest perceived that a loop-back connector was attached to port 2 and that a cross cable was used to connect ports 4 and 5.

Port Conversation

This test sends and receives data on the selected port. One way to run this test is to place a loop-back connector on the port to be tested and begin. Enter the number of the port and a baud rate (9600 is a typical value). Type some letters, and if the letters appear on the screen, the port is working. If the letters do not appear on the screen (which also occurs if the loop-back connector is removed), the port is not functioning correctly.

A second method that can be used to test the port is to connect it to a modem with a straight cable. Begin the test and type “at”. The modem should respond with “OK”, which will appear on the screen. Other commands can be sent to the modem or to any other serial device. Press Ctrl-Q to exit the terminal emulation test.

Test Signals Manually

This test confirms that signals are being sent and received on the selected port. Neither the loop-back connector nor the cross cable are necessary. Enter the number of the port to be tested and begin the test.

<table>
<thead>
<tr>
<th>State</th>
<th>DTR</th>
<th>DCD</th>
<th>DSR</th>
<th>RTS</th>
<th>CTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>ON</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OFF</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>

Figure 53: Initial test
Appendix D - Upgrades and Troubleshooting

First, type Ctrl-D to see the X in the DTR column move position, then type Ctrl-R to see the X in the RTS column change position. If each of the Xs moves in response to its command, the signals are being sent. Another method to test the signals is to use a loop-back connector. Enter the number of the port with the loopback connector and start the test. In this case, when Ctrl-D is typed, the Xs in the first three columns will move as shown below.

<table>
<thead>
<tr>
<th>State</th>
<th>DTR</th>
<th>DCD</th>
<th>DSR</th>
<th>RTS</th>
<th>CTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>ON</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>OFF</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>

*Figure 54: Second screen, showing changed positions*

This is because the test is receiving the DTR signal sent through the DCD and DSR pins. When Ctrl-R is typed, the Xs in the RTS and CTS columns should move together. If the Xs change position as described, the signals are being sent and received correctly.

**Test Analog Ports (for the TS110 only)**

This test consecutively reads the Analog-to-Digital converters on both analog ports and compares the variance between the current reading and the first reading (pattern). One way to run this test is to place a short-circuit connector on the ports. The reading should be at the bottom of the Analog-to-Digital scale. Another way is to place 10K ohms on the ports. The reading should be at half scale. A third way is to place no connector at all. The reading should be at full scale. Below is an example of the output screen, when using 10K ohms.

<table>
<thead>
<tr>
<th>ANALOG</th>
<th>Initial</th>
<th>Current</th>
<th>Correct</th>
<th>Passes</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>3fff</td>
<td>3fff</td>
<td>7</td>
<td>7</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>3fff</td>
<td>3fff</td>
<td>7</td>
<td>7</td>
<td>0</td>
</tr>
</tbody>
</table>

Press <ESC> to stop the test.
Appendix D - Upgrades and Troubleshooting

Test Digital Ports (for the TS110 only)

This test consecutively reads the digital ports and compares the variance between the current reading and the first reading (pattern). One way to run this test is to place a loop-back connector on the ports. The port reading on this condition should be 1. It means that pin+ and pin- have a closed loop. For the ports without loop-back, the reading should be 0. It means that pin+ and pin- have an open loop. Below is an example of the output screen. Digital ports 1, 2, 3, 4 and 5 have loop-back connectors. Digital ports 6, 7 and 8 have not.

<table>
<thead>
<tr>
<th>DIGITAL</th>
<th>Initial</th>
<th>Current</th>
<th>Correct</th>
<th>Passes</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>10</td>
<td>10</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>1</td>
<td>10</td>
<td>10</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>1</td>
<td>10</td>
<td>10</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>1</td>
<td>10</td>
<td>10</td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td>1</td>
<td>1</td>
<td>10</td>
<td>10</td>
<td>0</td>
</tr>
<tr>
<td>6</td>
<td>0</td>
<td>0</td>
<td>10</td>
<td>10</td>
<td>0</td>
</tr>
<tr>
<td>7</td>
<td>0</td>
<td>0</td>
<td>10</td>
<td>10</td>
<td>0</td>
</tr>
<tr>
<td>8</td>
<td>0</td>
<td>0</td>
<td>10</td>
<td>10</td>
<td>0</td>
</tr>
</tbody>
</table>

Press <ESC> to stop the test.

Single User Mode

The Cyclades-TS has a single user mode used when:

- The name or password of the user with root privileges is lost or forgotten,
- After an upgrade or downgrade which leaves the Cyclades-TS unstable,
- After a configuration change which leaves the Cyclades-TS inoperative or unstable.
Appendix D - Upgrades and Troubleshooting

Type the word “single” (with a blank space before the word) during boot using a console connection. This cannot be done using a telnet or other remote connection. The initial output of the boot process is shown below.

Entry Point = 0x00002120

loaded at: 00002120 0000D370
relocated to: 00300020 0030B270
board data at: 003052C8 0030537C
relocated to: 002FF120 002FF1D4
zimage at: 00008100 0006827E
relocated to: 00DB7000 00E1717E
initrd at: 0006827E 0024F814
relocated to: 00E18000 00FFF596
avail ram: 0030B270 00E18000

Linux/PPC load: root=/dev/ram

After printing “Linux/PPC load: root=/dev/ram,” the Cyclades-TS waits approximately 10 seconds for user input. This is where the user should type “<sp>single” (spacebar, then the word “single”). When the boot process is complete, the Linux prompt will appear on the console:

[root@(none) /]#

If the password or username was forgotten, execute the following commands:

passwd
saveconf
reboot
Appendix D - Upgrades and Troubleshooting

For configuration problems, you have two options:

**Step 1:** Edit the file(s) causing the problem with vi, then execute the commands:

```bash
saveconf
reboot
```

**Step 2:** Reset the configuration by executing the commands:

```bash
echo > /proc/flash/script
reboot
```

If the problem is due to an upgrade/downgrade, a second downgrade/upgrade will be necessary to reverse the process. First, the network must be initialized in order to reach a ftp server. Execute the following script, replacing the parameters with values appropriate for your system. If your ftp server is on the same network as the TS, the gw and mask parameters are optional.

```
config_eth0 ip 200.200.200.1 mask 255.255.255.0 gw 200.200.200.5
```

At this point, the DNS configuration (in the file `/etc/resolv.conf`) should be checked. Then, download the kernel image using the ftp command.

**Troubleshooting the Web Configuration Manager**

**What to do when the initial Web page does not appear**

Try pinging, telnetting, or tracerouting to the Cyclades-TS to make sure it is reachable. If not, the problem is probably in the network or network configuration. Are the interfaces up? Are the IP addresses correct? Are filters configured which block the packets? If the Cyclades-TS is reachable, see if the `/bin/webs` process is running by executing the command `ps`. If it is not, type `/bin/webs &` to start it. If the `/bin/webs` process is not being initialized during boot, change the file `/etc/inittab`.

**How to restore the Default Configuration of the Web Configuration Manager**

This would be required only when the root password was lost or the configuration file `/etc/websum.conf` was damaged. From a console or telnet session, edit the file `/etc/config_files`. Find the reference to `/etc/websum.conf` and delete it. Save the modified `/etc/config_files` file. Execute the command `saveconf`. Reboot the system. Enter into the Web Config-
configuration Manager with the default username and password (root/tslinux). Edit the file /etc/config_files and insert the reference to /etc/websum.conf.

Recover access to the Cyclades-TS110/100 console port

There is no dedicated console port available in the Cyclades-TS110/100. As factory default the serial port is set to work as a console port to allow initial product configuration. After that, changes can still be made through the Ethernet port and a Telnet command. If for some reason this access is lost (usually misconfiguration), the product can only be configured if the steps bellow are followed.

**Step 1:** Power the Cyclades-TS110/100 off.

**Step 2:** Connect the Cyclades-TS110/100 to a terminal configured to work at 9600 bps, with 8 bits, no parity and 1 stop bit.

**Step 3:** Press and hold the ADM button and power on the Cyclades-TS110/100.

There’s a small hole in the box containing an internal ADM button that can be reached by a thin, sharp object.

**Step 4:** Release the ADM button when the self test starts on the terminal’s screen.

The Cyclades-TS110/100 be now in single user mode, the serial port will work as a console port and the product can be reconfigured. Notice that no previous configuration is lost. After finishing, save the configuration (saveconf), power the Cyclades-TS110/100 off, and reconnect the original device to the serial port.

**Using a different speed for the Serial Console**

The serial console is originally configured to work at 9600 bps. If you want to change that, it is necessary to change the configuration following the steps:

**Step 1:** Run bootconf. The user will be presented with the screen:

Current configuration

MAC address assigned to Ethernet [00:60:2e:00:16:b9]

IP address assigned to Ethernet interface [192.168.160.10]

Watchdog timer ((A)ctive or (I)nactive) [A]

Firmware boot from ((F)lash or (N)etwork) [F]
Appendix D - Upgrades and Troubleshooting

Boot type ((B)oottp, (T)ftp or Bot(H)) [T]
Boot File Name [zvmppctsbin]
Server's IP address [192.168.160.1]
Console speed [9600]
(P)erform or (S)kip Flash test [P]
(S)kip, (Q)uick or (F)ull RAM test [F]
Fast Ethernet ((A)uto Neg, (1)00 BtH, 100 Bt(F), 10 B(t)F, 10 Bt(H)) [A]
Fast Ethernet Maximum Interrupt Events [0]

Type <Enter> for all fields but the Console Speed. When presented the following line:

Do you confirm these changes in flash ( (Y)es, (N)o (Q)uit ) [N] :

Step 2: Enter Y and the changes will be saved in flash.

Step 3: Logout and login again to use the console at the new speed.
Appendix D - Upgrades and Troubleshooting

CPU LED

Normally the CPU status LED should blink consistently one second on, one second off. If this is not the case, an error has been detected during the boot. The blink pattern can be interpreted via the following table:

<table>
<thead>
<tr>
<th>Event</th>
<th>CPU LED Morse code</th>
</tr>
</thead>
<tbody>
<tr>
<td>Normal Operation</td>
<td>S (short, short, short . . . )</td>
</tr>
<tr>
<td>Flash Memory Error - Code</td>
<td>L (long, long, long . . . )</td>
</tr>
<tr>
<td>Flash Memory Error - Configuration</td>
<td>S, L</td>
</tr>
<tr>
<td>Ethernet Error</td>
<td>S, S, L</td>
</tr>
<tr>
<td>No Interface Card Detected</td>
<td>S, S, S, L</td>
</tr>
<tr>
<td>Network Boot Error</td>
<td>S, S, S, L</td>
</tr>
<tr>
<td>Real-Time Clock Error</td>
<td>S, S, S, S, L</td>
</tr>
</tbody>
</table>

Note: The Ethernet error mentioned in the above table will occur automatically if the Fast Ethernet link is not connected to an external hub during the boot. If the Fast Ethernet is not being used or is connected later, this error can be ignored.
Appendix E - Certificate for HTTP Security

Introduction

The following configuration will enable you to obtaining a Signed Digital Certificate. A certificate for the HTTP security is created by a CA (Certificate Authority). Certificates are most commonly obtained through generating public and private keys, using a public key algorithm like RSA or X509. The keys can be generated by using a key generator software.

Procedure

Step 1: Enter OpenSSL command.

On a Linux computer, key generation can be done using the OpenSSL package, through the following command:

```
# openssl req -new -nodes -keyout private.key -out public.csr
```

If this command is used, the following information is required:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Country Name (2 letter code) [AU]:</td>
<td>The country code consisting of two letters.</td>
</tr>
<tr>
<td>State or Province Name (full name) [Some-State]:</td>
<td>Provide the full name (not the code) of the state.</td>
</tr>
<tr>
<td>Locality Name (e.g., city) []:</td>
<td>Enter the name of your city.</td>
</tr>
<tr>
<td>Organization Name (e.g., company) [Internet Widgits Ltd]:</td>
<td>Organization that you work for or want to obtain the certificate for.</td>
</tr>
<tr>
<td>Organizational Unit Name (e.g., section) []:</td>
<td>Department or section where you work.</td>
</tr>
<tr>
<td>Common Name (e.g., your name or your server’s hostname) []:</td>
<td>Name of the machine where the certificate must be installed.</td>
</tr>
</tbody>
</table>
Appendix E - Certificate for HTTP Security

Table 42: Required information for the OpenSSL package

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email Address []:</td>
<td>Your email address or the administrator’s email address.</td>
</tr>
</tbody>
</table>

The other requested information can be skipped.

The certificate signing request (CSR) generated by the command above contains some personal (or corporate) information and its public key.

Step 2: Submit CSR to the CA.

The next step is to submit the CSR and some personal data to the CA. This service can be requested by accessing the CA Web site and is not free. There is a list of CAs at the following URL

pki-page.org

The request will be analyzed by the CA, for policy approval and to be signed.

Step 3: Upon receipt, install certificate.

After the approval, the CA will send a certificate file to the origin, which we will call Cert.cer, for example purposes. The certificate is also stored on a directory server. The certificate must be installed in the GoAhead Web server, by following these instructions:

Step A: Open a Cyclades Terminal Server session and do the login.

Step B: Join the certificate with the private key into the file /web/server.pem.

    #cat Cert.cer private.key > /web/server.pem

Step C: Copy the certificate to the file /web/cert.pem.

    #cp Cert.cer /web/cert.pem

Step D: Include the files /web/server.pem and /web/cert.pem in /etc/config_files.
Appendix E - Certificate for HTTP Security

Step E: Save the configuration in flash.

#saveconf

Step F: The certification will be effective in the next reboot.
This page has been left intentionally blank.
Appendix F - Web User Management

Introduction

In the Cyclades-TS Web server, the user database is completely separated from the system’s (as defined in the /etc/passwd file), and the logic used for managing permissions is also different. The Web’s user database is stored in the /etc/websum.conf file, and it has basically three lists: users, user groups and access limits.

Default Configuration for Web User Management

The following three screen shots show the default configuration for User List, User Group List, and Access Limit List pages, respectively.

![Figure 55: User List default page](image1)

![Figure 56: User Group List default page](image2)
## Appendix F - Web User Management

### Access Limit List

<table>
<thead>
<tr>
<th>Entry</th>
<th>URL</th>
<th>Privilege Level</th>
<th>Access Method</th>
<th>Secure</th>
</tr>
</thead>
<tbody>
<tr>
<td>/</td>
<td>USER</td>
<td>FULL</td>
<td></td>
<td>No</td>
</tr>
<tr>
<td>/appl/</td>
<td>USER</td>
<td>COOKIE</td>
<td></td>
<td>No</td>
</tr>
<tr>
<td>/read/</td>
<td>MONITOR</td>
<td>COOKIE</td>
<td></td>
<td>No</td>
</tr>
<tr>
<td>/adm/</td>
<td>ADMINISTRATOR</td>
<td>COOKIE</td>
<td></td>
<td>No</td>
</tr>
<tr>
<td>/cfg/</td>
<td>FULL</td>
<td>COOKIE</td>
<td></td>
<td>No</td>
</tr>
<tr>
<td>/umi/</td>
<td>FULL</td>
<td>COOKIE</td>
<td></td>
<td>No</td>
</tr>
<tr>
<td>/goform/</td>
<td>MONITOR</td>
<td>COOKIE</td>
<td></td>
<td>No</td>
</tr>
<tr>
<td>/goform/Login</td>
<td>USER</td>
<td>FULL</td>
<td></td>
<td>No</td>
</tr>
<tr>
<td>/goform/CheckLogin</td>
<td>USER</td>
<td>FULL</td>
<td></td>
<td>No</td>
</tr>
<tr>
<td>/goform/MainPageTable</td>
<td>USER</td>
<td>COOKIE</td>
<td></td>
<td>No</td>
</tr>
<tr>
<td>/goform/Logout</td>
<td>USER</td>
<td>COOKIE</td>
<td></td>
<td>No</td>
</tr>
<tr>
<td>/goform/appl/</td>
<td>USER</td>
<td>COOKIE</td>
<td></td>
<td>No</td>
</tr>
<tr>
<td>/goform/adm/</td>
<td>ADMINISTRATOR</td>
<td>COOKIE</td>
<td></td>
<td>No</td>
</tr>
<tr>
<td>/goform/cfg/</td>
<td>FULL</td>
<td>COOKIE</td>
<td></td>
<td>No</td>
</tr>
<tr>
<td>/goform/umi/</td>
<td>FULL</td>
<td>COOKIE</td>
<td></td>
<td>No</td>
</tr>
</tbody>
</table>

*Figure 57: Access Limit List default page*
Appendix F - Web User Management

How Web User Management works

When a user logs in, the username and the password are encrypted and stored in the browser. Whenever a URL is requested, the User Manager will perform the following tasks:

Task 1: Check the URL in the Access Limit List

The Web server first scans for the full URL, and then it looks for the subdirectories, until reaching the root directory “/.” (In the URL http://CAS/goformcfg/IPTablesRulesHandle, the access limits will be scanned in the following order: /goformcfg/IPTablesRulesHandle, /goformcfg, /goform and /.) When the URL matches an Access Limit, the following information will be available:

Accessibility
When configured as FULL ACCESS, the URL can be accessed without any authentication; otherwise, the user can authenticate with BASIC, DIGEST or COOKIE authentication. The last type is recommended, because it allows the user to log out in the end of the session. The page will not be accessible when the accessibility is configured as NO ACCESS.

Security
When set to be secure, the page will be accessed only through HTTPS, which will encrypt the pages through OpenSSL. If the browser is in unsecure mode, the protocol and the port will change to HTTPS.

Privilege
This is the level of accessibility of the page. If the privilege is USER, any user will be able to access the page. If the privilege is FULL, only users with full access will be able to access the page. There are two levels between them: MONITOR and ADMINISTRATOR.
Appendix F - Web User Management

Task 2: Read the Username and the Password
This is done when the page must be accessed through authentication. If the username matches an entry in the users list, the following information will be available:

- **Enabled** The username must be enabled to be authenticated.
- **Encrypted password** The password passed by the browser must match the one registered in the entry.
- **Group** Each username is linked to a user group.

Task 3: Look for the group retrieved in the user groups list
The user group entry will have the following information:

- **Enabled** The group must be enabled to grant access to the URL.
- **Privilege** The group can have four privileges: in increasing order, they are USER, MONITOR, ADMINISTRATOR and FULL. The group privilege will be compared with the URL privilege. If it is greater or equal, the URL can be accessed by the user; otherwise, access is denied.

Web User Management Configuration - Getting Started

The users, groups and access limits for Web User Management are configurable with your browser, though it is not recommended to change the groups and the access limits. In the default configuration:

- The access limits have privileges based on the functionality of the Web page.
- There are four different groups (root, monitor, admin and user), each one with a specific privilege.
- There is one root user (username is root and password is tslinux).
Appendix F - Web User Management

Changing the Root Password

The first thing to do after logging into a Web session the first time must be to change the root password. See Security Issue under Figure 11: Configuration & Administration Menu page.

Step 1: Click on the link Web User Management > Users.

Step 2: Select the root user and click the Change Password button.

Step 3: Type the password twice and click the Submit button.

Step 4: Click on the link Web User Management > Load/Save Web Configuration.

The Login page will appear.

Step 5: Type the username root and the password that was configured, then click on the Login button.

Step 6: After the authentication, click on the Save Configuration button.

Step 7: Click on the link Administration > Load/Save Configuration.

Step 8: Click on the Save to Flash button.

Adding and Deleting Users

Adding a User

Step 1: Click on the link Web User Management > Users.

Step 2: Click on the Add User button.

Step 3: Configure the new user.

Type the username, the password (twice) and select a user group, depending on the access privilege desired. Leave the item Enabled checked.
Appendix F - Web User Management

Step 4: Click on the Submit button.
A confirmation message will appear.

Step 5: If there are more users to be added, repeat the steps 1 to 4.

Step 6: Click on the link Web User Management > Load/Save Web Configuration.

Step 7: Click on the Save Configuration button.
This will save the users added in the file /etc/websum.conf.

Step 8: Click on the link Administration > Load/Save Configuration.

Step 9: Click on the Save to Flash button.

Step 10: Test the user(s) added.
Log out the current user (Go to the link Application > Logout) and log in again, with the new user.

Deleting a User

The root user is delete-protected, and, because of that, it cannot be removed from the user list. The other users can be deleted.

Step 1: Click on the link Web User Management > Users.

Step 2: Select the user to be deleted and click on the Delete User button.
A confirmation message will appear.

Step 3: If there are more users to be deleted, repeat the steps 1 and 2.

Step 4: Click on the link Web User Management > Load/Save Web Configuration.

Step 5: Click on the Save Configuration button.
This will save the users added in the file /etc/websum.conf

Step 6: Click on the link Administration > Load/Save Configuration.

Step 7: Click on the Save to Flash button.
Appendix F - Web User Management

Adding and Deleting User Groups

The default configuration already comes with four user groups, and, for most of the cases, they will be enough. However, you have the option of editing the user groups.

Adding a group

Step 1: Click on the link Web User Management > Groups.

Step 2: Click on the Add Group button

Step 3: Configure the new group.
Type the group name and select the access privilege this group will have. Leave the Enabled item checked.

Step 4: Click on the Submit button.
A confirmation message will appear.

Step 5: If there are more groups to be added, repeat the steps 1 to 4.

Step 6: Click on the link Web User Management > Load/Save Web Configuration.

Step 7: Click on the Save Configuration button.
This will save the users added in the file /etc/websum.conf

Step 8: Click on the link Administration > Load/Save Configuration.

Step 9: Click on the Save to Flash button.

Deleting a group

Before deleting a group, make sure that there are no users using that group.

Step 1: Click on the link Web User Management > Groups.

Step 2: Select the group to be deleted and click on the Delete Group button.
A confirmation message will appear.
Appendix F - Web User Management

Step 3: If there are more groups to be deleted, repeat the steps 1 and 2.

Step 4: Click on the link Web User Management > Load/Save Web Configuration.

Step 5: Click on the Save Configuration button.
   This will save the users added in the file /etc/websum.conf

Step 6: Click on the link Administration > Load/Save Configuration.

Step 7: Click on the Save to Flash button.

Adding and Deleting Access Limits

The default configuration has the access limits set according to the functionality of the Web page.

- Pages or forms which causes the configuration to change will have FULL privilege (only high-privileged users will have access to it).
- Pages which change the status of the board without changing the configuration will have ADMINISTRATOR privilege;
- Pages with the system information will have MONITOR privilege.
- Only application pages will have USER privilege.

Changing access limits is not recommended, unless you need to create or change the web server pages; even so, the user should place the web pages in the subdirectories with the privilege desired. For example, a page with ADMINISTRATOR privilege should be placed in /adm.

Adding an Access Limit

Step 1: Click on the link Web User Management > Access Limits.

Step 2: Click on the Add Access Limit button.
Appendix F - Web User Management

Step 3: Configure the new access limit.
Type the URL (or the subdirectory), and select the access privilege. If authentication is required to access the page, select COOKIE ACCESS; otherwise, select FULL ACCESS. If this page is confidential, check the Secure box.

Step 4: Click on the Submit button.
A confirmation message will appear.

Step 5: If there are more access limits to be added, repeat the steps 1 to 4.

Step 6: Click on the link Web User Management > Load/Save Web Configuration.

Step 7: Click on the Save Configuration button.
This will save the users added in the file /etc/websum.conf.

Step 8: Click on the link Administration > Load/Save Configuration.

Step 9: Click on the Save to Flash button.

Deleting an access limit

Step 1: Click on the link Web User Management > Access Limits.

Step 2: Select the access limit to be deleted and click on the Delete Access Limit button.
A confirmation message will appear.

Step 3: If there are more access limits to be deleted, repeat the steps 1 and 2.

Step 4: Click on the link Web User Management > Load/Save Web Configuration.

Step 5: Click on the Save Configuration button.
This will save the users added in the file /etc/websum.conf

Step 6: Click on the link Administration > Load/Save Configuration.

Step 7: Click on the Save to Flash button.
Appendix F - Web User Management

This page has been left intentionally blank.
Appendix G - Connect to Serial Ports from Web

Introduction

Depending on how the serial port is configured, connecting to a serial port will either open up a telnet or ssh connection. A serial port configured as socket_server or raw_data will open up a telnet connection while socket_ssh will open up a ssh connection. Any Web user configured in the Web User Management section of the WMI will be able to use this application.

Tested Environment

Table 43: Windows XP + JREv1.4.0_01 or 02

<table>
<thead>
<tr>
<th>Browser</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet Explorer 6.0</td>
<td>Success</td>
</tr>
<tr>
<td>Netscape 6/6.2.3</td>
<td>Success</td>
</tr>
<tr>
<td>Netscape 7.0</td>
<td>Success</td>
</tr>
<tr>
<td>Mozilla 1.1</td>
<td>Success</td>
</tr>
</tbody>
</table>

Requirements: Java 2 Runtime Environment (JRE) SE v1.4.0_01 or v1.4.0_02 (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.
Appendix G - Connect to Serial Ports from Web

On Windows

From 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 v1.4.0 ...”. 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 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.
Appendix G - Connect to Serial Ports from Web

Step-by-Step Process

Step 1: **Point your browser to the Console Server.**

In the address field of your browser type the Console Access Server’s IP address. For example:

http://10.0.0.0

Step 2: **Log in.**

Log in with a user configured in the Web User Management section, and its password. This will take you to the Configuration and Administration page.

Step 3: **Select the Connect to Serial Ports link.**

Click on the Connect to Serial Ports link on the Link Panel to the left of the page in the Configuration section. This will take you to the Port Selection page. The ports will be listed by their server farm name if it were configured.

![Serial Port Connection](image)

*Figure 58: Serial Port Connection page*

Step 4: **Select port.**

On the Port Selection page, choose a port to connect to from the dropdown menu and click the Connect button. This will open a new browser window that contains the applet connecting to the server chosen.
Appendix G - Connect to Serial Ports from Web

Figure 59: Port Connection page
At the upper right hand corner of the window, the left icon is a refresh button. Clicking on that button will reconnect to the server.

Figure 60: The Refresh button
The right icon closes the window. At the upper left corner, the server name is shown. In this case, the user didn't configure the serverfarm name, so "Port 1" appears.

Step 5: Log in.
If the port selected was configured as socket_server or raw_data, and depending on how it is configured to be authenticated, log in by typing into the terminal.

If the port selected was configured for a ssh connection, a Login window will pop
Appendix G - Connect to Serial Ports from Web

up. If you don't see it pop up, check your taskbar. Enter in the username and the username's password.

Enter in the username and the username's password if the servers were configured for authentication. If no authentication is configured, then just click Cancel.

![SSH User Authentication Popup Window](image)

*Figure 61: SSH User Authentication Popup Window*

**Step 6: Enter command.**

Click in the terminal window and start entering commands.

**Step 7: To send a break to the terminal.**

Click on the SendBreak button.

**Step 8: Disconnect connection.**

Click on the Disconnect button. Make sure the Status bar shows an Offline status. Closing the popup window will also disconnect you from the server.

**Step 9: Reconnect to port.**

Refresh the current page by clicking on the refresh icon at the upper right hand corner of the window.
Appendix G - Connect to Serial Ports from Web

This page has been left intentionally blank.
Appendix H - Examples for Config Testing

Introduction

The following three examples are just given to test a configuration. The steps should be followed after configuring the Cyclades-TS.

Console Access Server

With the Cyclades-TS set up as a CAS you can access a server connected to the Cyclades-TS through the server’s serial console port from a workstation on the LAN or WAN. There is no authentication by default, but the system can be configured for authentication to be performed by a Radius server, a TacacsPlus server, or even by a local database. Either telnet or ssh can be used.

See Appendix A - New User Background Information for more information about ssh. The instructions in Chapter 2 - Installation, Configuration, and Usage will set up a fully-functional, default CAS environment. More options can be added after the initial setup, as illustrated in Chapter 3 - Additional Features.

An example of a CAS environment is shown in the following figure. Figure 62: Console Access Server diagram. This configuration example has local authentication, an Ethernet interface provided by a router, and serially-connected workstations.
Appendix H- Examples for Config Testing

The following diagram Figure 62: Console Access Server diagram, shows additional scenarios for the Cyclades-TS: both remote and local authentication, data buffering, and remote access.
Appendix H- Examples for Config Testing

As shown in the above figure, our “CAS with local authentication” scenario has either telnet or ssh (a secure shell session) being used. After configuring the serial ports as described in Chapter 3 - Additional Features or in Appendix C - The pslave Configuration File, the following step-by-step check list can be used to test the configuration.

Figure 63: CAS diagram with various authentication methods

User Guide
Step 1: Create a new user.
Run the `adduser <username>` to create a new user in the local database. Create a password for this user by running `passwd <username>`.

Step 2: Confirm physical connection.
Make sure that the physical connection between the Cyclades-TS and the servers is correct. A cross cable (not the modem cable provided with the product) should be used. Please see Appendix B - Cabling, Hardware, and Electrical Specifications for pin-out diagrams.

Step 3: Confirm that server is set to same parameters as the TS.
The Cyclades-TS has been set for communication at 9600 bps, 8N1. The server must also be configured to communicate on the serial console port with the same parameters.

Step 4: Confirm routing.
Also make sure that the computer is configured to route console data to its serial console port (Console Redirection).

Step 5: Telnet to the server connected to port 1.
From a server on the LAN (not from the console), try to telnet to the server connected to the first port of the Cyclades-TS using the following command:
```
telnet 200.200.200.1 7001
```
For both telnet and ssh sessions, the servers can be reached by either:

1. Ethernet IP of the Cyclades-TS and assigned socket port.

or

2. Individual IP assigned to each port.

If everything is configured correctly, a telnet session should open on the server connected to port 1. If not, check the configuration, follow the steps above again, and check the troubleshooting appendix.
Step 6: Activate the changes.

Now continue on to Task 5: Activate the changes through listed in Chapter 2 - Installation, Configuration, and Usage.

**Note:** It is possible to access the serial ports from Microsoft stations using some off-the-shelf packages. Although Cyclades is not liable for those packages, successful tests were done using at least one of them. From the application’s viewpoint running on a Microsoft station, the remote serial port works like a regular COM port. All the I/O with the serial device attached to the Cyclades-TS is done through socket connections opened by these packages and a COM port is emulated to the application.

**Terminal Server**

The Cyclades-TS provides features for out-of-band management via the configuration of terminal ports. All ports can be configured as terminal ports. This allows a terminal user to access a server on the LAN. The terminal can be either a dumb terminal or a terminal emulation program on a PC.

![Terminal Server diagram](image)

**Figure 64: Terminal Server diagram**

No authentication is used in the example shown above and rlogin is chosen as the protocol. After configuring the serial ports as described in Chapter 3 - Additional Features or in Appendix C - The pslave Configuration File, the following step-by-step check list can be used to test the configuration.
Appendix H- Examples for Config Testing

Step 1: Create a new user.
Since authentication was set to none, the Cyclades-TS will not authenticate the user. However, the Linux Server receiving the connection will. Create a new user on the server called test and provide him with the password test.

Step 2: Confirm that the server is reachable.
From the console, ping 200.200.200.3 to make sure the server is reachable.

Step 3: Check physical connections.
Make sure that the physical connection between the Cyclades-TS and the terminals is correct. A cross cable (not the modem cable provided with the product) should be used. Please see the Appendix B - Cabling, Hardware, and Electrical Specifications for pin-out diagrams.

Step 4: Confirm that terminals are set to same parameters as the TS.
The Cyclades-TS has been set for communication at 9600 bps, 8N1. The terminals must also be configured with the same parameters.

Step 5: Log onto server with new username and password.
From a terminal connected to the Cyclades-TS, try to login to the server using the username and password configured in step one.

Step 6: Activate changes.
Now continue on to Task 5: Activate the changes through listed in Chapter 2 - Installation, Configuration, and Usage.
Dial-in Access

The Cyclades-TS can be configured to accommodate out-of-band management. Ports can be configured on the Cyclades-TS to allow a modem user to access the LAN. Radius authentication is used in this example and ppp is chosen as the protocol on the serial (dial-up) lines. Cyclades recommends that a maximum of two ports be configured for this option.

Figure 65: Ports configured for Dial-in Access

After configuring the serial ports as described in Chapter 3 - Additional Features or in Appendix C - The pslave Configuration File, the following step-by-step check list can be used to test the configuration.

**Step 1: Create a new user.**

Since Radius authentication was chosen, create a new user on the Radius authentication server called test and provide them with the password test.
Step 2: **Confirm that the Radius server is reachable.**
From the console, ping 200.200.200.2 to make sure the Radius authentication server is reachable.

Step 3: **Confirm physical connections.**
Make sure that the physical connection between the Cyclades-TS and the modems is correct. The modem cable provided with the product should be used. Please see Appendix B - Cabling, Hardware, and Electrical Specifications for pinout diagrams.

Step 4: **Confirm modem settings.**
The Cyclades-TS has been set for communication at 57600 bps, 8N1. The modems should be programmed to operate at the same speed on the DTE interface.

Step 5: **Confirm routing.**
Also make sure that the computer is configured to route console data to the serial console port.

Step 6: **Perform a test dial-in.**
Try to dial in to the Cyclades-TS from a remote computer using the username and password configured in step one. The computer dialing in must be configured to receive its IP address from the remote access server (the Cyclades-TS in this case) and to use PAP authentication.

Step 7: **Activate changes.**
Now continue on to Task 5: Activate the changes through Task 8: Reboot the Cyclades-TS listed in Chapter 2 - Installation, Configuration, and Usage.
Appendix I - Billing Feature

Introduction

All the Cyclades TS family can also be simply used as an intermediate buffer to collect serial data (like billing tickets from a PABX), making them available for a posterior file transfer. Different ports can now simultaneous "billing sessions".

General Feature Description

The Cyclades-TS reads the serial port and saves information to Ramdisk files, limited to a maximum number of records per file or a maximum lifetime. After they are closed, these files are available for file transfer at /var/run/DB.

Configuration

The plsave.conf file has one more “protocol” and three new parameters shown on the Data Buffering section of the Web interface. They are:

```
all.protocol
all.billing_records
all.billing_timeout
all.billing_eor
```

```
billing
50
60 (min)
"\n"
```

Note: All presented values above are going to implement the billing feature for ALL ports of the product. If the configuration for a specific port is required, all related parameters beginning with all must be changed to S.x, where x is the number of the port to be configured.
How it works

Once the cy_ras program detects the protocol as “billing,” it starts the billing application. The billing application then opens the port (as configured in pslave.conf) and starts reading it. Records terminated by "billing_eor string" are expected to be received. The Cyclades TS doesn’t change the termination method, transferring the same sequence to the file. The name of the temporary file used to write these records is:

cycXXXXX-YYMMDD.hhmmss.tmp

where:

- XXXXX is the “hostname” or “serverfarm”
- YYMMDD is the year/month/day
- hhmmss is the hour:min:sec

This name helps the user archive and browse their directory as the file can be chronologically listed, not based on its creation or modification times, but based on when its contents were recorded. Also, whenever “hostname” is not significant, the user can use the “serverfarm” name (s1.serverfarm in pslave.conf) to match their actual plant (like PABX-trunk9). The temporary file described above is closed and renamed to cycXXXXX-YYMMDD.hhmmss.txt and a new temporary file is opened when:

1. The maximum number of records specified by “billing_records” is reached;
2. The lifetime specified by “billing_timeout” finishes.

If no record is received within a file lifetime period, no file will be actually saved.

**Note:** A zero-value for “billing_records” stops the application and a zero-value for “billing_timeout” means no timeout is desired and so the file will only be closed after “billing_records” are received.
Appendix I - Billing Feature

Billing Configuration Script

The `config_billing.sh` script configures everything related to billing. The user can set a port as billing protocol, configure automatic upload of files and enlarge the ramdisk space. The user can also configure this feature by editing the parameters in the `/etc/billing_up.conf` file. If the script is executed, it will ask for parameters and configure the `billing_up.sh` according to the options, and set the `/etc/crontabBilling` and `/etc/crontab_files` to upload the file periodically. The user must set these parameters:

- Upload Protocol Mode (ftp or scp)
- Local directory
- IP address of remote server
- Remote directory
- Upload interval
- User
- Password

The major script is `config_billing.sh`. This script configures a port to billing protocol, can be used to enlarge the ramdisk space and configure upload scripts, by ftp or ssh.

To configure a port for billing, you can run `config_billing.sh` and pass the parameters that need to be configured. The syntax of the command is as follows:

```
# config_billing.sh [X] [options]
```

where:

- X is the port's number which is configured

`[options]` can be:

- `-s` - speed
- `-d` - data size
- `-b` - stopbit
- `-p` - parity
- `-r` - billing records
Appendix I - Billing Feature

- `-e` - billing EOR (this parameter must be around " ", for example "\n")
- `-D` - billing dir
- `-S` - serverFarm
- `-t` - time date of system
- `-T` - timeout
- `-i` - ip of the TS box
- `-n` - netmask of the TS box
- `-R` - default route of the TS box
- `-u` - configure upload_scripts
- `-l` - enlarge ramdisk

If the `-u` option is passed, the script will prompt a sequencial menu, to configure some parameters. The parameters that are going to be asked are the following:

- Transfer Mode (ftp or scp)
- Local Directory [/var/run/DB]
- Remote server IP
- User
- Password
- Upload Interval in minutes

If scp mode is choosen and a key for authentication is not present, the script will generate it and try to upload it to the server. The key must be stored on the server with the appropriate configuration.

After all changes, run `saveconf` and restart the box to activate options related to upload and ramdisk enlargement.

### Disk Space Issue

Finally, it is important to note that there is a protection against disk space problems. If you configure flow control to “hardware” for the serial port (`all.flow = hard` in the pslave.conf file), the application monitors the available disk space and if it is less than 100 Kb, the serial interface deactivates “RTS” signal on the RS-232. “RTS” is reactivated once the disk free space is greater than 120 Kb.
## Appendix J - Wiz Application Parameters

### Basic Parameters (wiz)

- Hostname
- System IP
- Domain Name
- DNS Server
- Gateway IP
- Network Mask

### Access Method Parameters (wiz --ac <type>)

(CAS profile)
- Ipno
- Socket_port
- Protocol
- Modbus_smode
- Users
- Poll_interval
- Tx_interval
- Idletimeout
- Conf.group
- <sN>.serverfarm
- pool_ipno
- pool_socket_port
Appendix J - Wiz Application Parameters

- pool_serverfarm
- web_WinEMS
- translation

(TS profile)
- Protocol
- Socket_port
- Userauto
- Telnet_client_mode

Alarm Parameter (wiz --al)

- Alarm
- xml_monitor

Authentication Parameters (wiz --auth)

- Authtype
- Authhost1
- Accthost1
- Authhost2
- Accthost2
- Radtimeout
Appendix J - Wiz Application Parameters

- Radretries
- Secret

**Data Buffering Parameters (wiz --db)**

- Data_buffering
- Conf.nfs_data_buffering
- Syslog_buffering
- Dont_show_DBmenu
- DB_timestamp
- DB_mode
- Syslog_sess

**Power Management Parameters (wiz --pm)**

- pmkey
- pmNumOfOutlets
- pmoutlet
- pmtype
- pmusers
Appendix J - Wiz Application Parameters

Serial Settings Parameters (wiz --sset <type>)

(CAS profile)
- Speed
- Datasize
- Stopbits
- Parity
- Flow
- Dcd
- SttyCmd
- DTR_reset

(TS profile)
- Speed
- Datasize
- Stopbits
- Parity
- Flow
- Dcd
Sniffing Parameters (wiz --snf)

- Admin_users
- Sniff_mode
- Escape_char
- Multiple_sessions

Syslog Parameters (wiz --sl)

- Conf.facility
- Conf.DB_facility

Terminal Appearance Parameters (wiz --tl)

- Issue
- Prompt
- Lf_suppress
- Auto_answer_input
- Auto_answer_output
Appendix J - Wiz Application Parameters

Terminal Server Profile Other Parameters (wiz --tso)

- Host
- Term
- Conf.locallogins
Appendix K - Copyrights

References

The Cyclades-TS is based in the HardHat Linux distribution, developed by Montavista Software for embedded systems. Additionally, several other applications were incorporated into the product, in accordance with the free software philosophy.

The list below contains the packets and applications used in the Cyclades-TS and a reference to their maintainers. The copyrights notices required in some packets are placed in the /COPYRIGHTS directory of the Cyclades-TS image.

**Bootparamd**

NetKit Bootparamd version 0.17  
ftp://ftp.uk.linux.org/pub/linux/Networking/netkit

**Busybox**

BusyBox version 0.60.2  

**Cron**

Paul Vixie's cron version 3.0.1.  
paul@vix.com

**DHPCCD**

http://www.phystech.com/download/dhcpd.html

**Flex**

Flex version 2.5.4  
vern@ee.lbl.gov  
COPYRIGHT: This product includes software developed by the University of California, Berkeley and its contributors
Appendix K - Copyrights

GNU
The GNU project
http://www.gnu.org

HardHat Linux
MontaVista Software - HardHat version 1.2
http://www.montavista.com

IPChains
Netfilter IPChains version 1.3.9. Extracted from the HardHat Linux
http://www.netfilter.org

Linux Kernel
Linux Kernel version 2.2.17. Extracted from the HardHat Linux distribution
http://www.kernel.org

NTP
NTP client
http://doolittle.faludi.com/ntpclient/

OpenSSH
OpenSSH version 3.5p1
http://www.openssh.org
COPYRIGHT: This product includes software developed by the University of California, Berkeley and its contributors.

OpenSSL
OpenSSL Project version 0.9.6g
http://www.openssl.org
COPYRIGHT: This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)
COPYRIGHT: This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)
Appendix K - Copyrights

PAM
Linux PAM version 0.75
http://www.kernel.org/pub/linux/libs/pam/

Portslave
SourceForge Portslave project version 2000.12.25. (modified). Includes pppd version 2.4.1 and rlogin version 8.10
http://sourceforge.net/projects/portslave/

RSYNC
rsync version 2.5.5
http://rsync.samba.org/rsync/

Syslog-ng
Syslog new generation version 1.5.17
http://www.balabit.hu/products/syslog-ng/

Tinylogin
TinyLogin version 0.80

WEBS
GoAhead WEBS version 2.1 (modified)
http://goahead.com/webserver/webserver.htm
Copyright (c) 20xx GoAhead Software, Inc. All Rights Reserved

ZLIB
zlib version 1.1.4
http://www.gzip.org/zlib/
This page has been left intentionally blank.
List of Figures

1. Cable Package #1 .......................................................... 20
2. Cable Package #2 .......................................................... 21
3. The Cyclades-TS3000 and cables .................................... 22
4. The Cyclades-TS2000 and cables .................................... 23
5. The Cyclades-TS1000 and cables .................................... 24
6. The Cyclades-TS800 and cables .................................... 25
7. The Cyclades-TS400 and cables .................................... 26
8. The Cyclades-TS110 and cables .................................... 27
9. The Cyclades-TS100 and cables .................................... 28
10. Login page of Web Configuration Manager ....................... 48
11. Configuration & Administration Menu page ...................... 49
12. General page ............................................................ 50
13. Choose a free COM port ............................................... 61
14. Port Settings ............................................................ 62
15. The /etc/hostname file with hostname typed in ............... 64
16. Contents of the /etc/hosts file .................................... 64
17. Configuration and Administration page ......................... 88
18. Port Selection page .................................................... 89
19. Serial Port Configuration page ..................................... 89
20. Profile Section of Serial Port Configuration page .............. 90
21. Serial Ports - Users Group Table Entry page .................... 91
22. Example of Centralized Management ............................. 129
23. An example using the Clustering feature ......................... 133
24. Edit Text File page .................................................... 140
<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>25</td>
<td>Data Buffering section of the Serial Port Configuration page</td>
<td>145</td>
</tr>
<tr>
<td>26</td>
<td>Data Buffering section of the General page</td>
<td>146</td>
</tr>
<tr>
<td>27</td>
<td>DHCP client section</td>
<td>158</td>
</tr>
<tr>
<td>28</td>
<td>IP Chain filtering</td>
<td>160</td>
</tr>
<tr>
<td>29</td>
<td>Modbus application</td>
<td>185</td>
</tr>
<tr>
<td>30</td>
<td>Sniff Session section of the Serial Port Configuration page</td>
<td>218</td>
</tr>
<tr>
<td>31</td>
<td>Syslog page 1</td>
<td>234</td>
</tr>
<tr>
<td>32</td>
<td>Data flow diagram of Linux-PAM</td>
<td>273</td>
</tr>
<tr>
<td>33</td>
<td>Configuration diagram</td>
<td>293</td>
</tr>
<tr>
<td>34</td>
<td>Power Management page</td>
<td>313</td>
</tr>
<tr>
<td>35</td>
<td>Power Management page after turning outlet 1 on</td>
<td>314</td>
</tr>
<tr>
<td>36</td>
<td>Power Management page after locking outlet 1</td>
<td>315</td>
</tr>
<tr>
<td>37</td>
<td>Cable 1 - Cyclades RJ-45 to DB-25 Male, straight-through</td>
<td>350</td>
</tr>
<tr>
<td>38</td>
<td>Cable 2 - Cyclades RJ-45 to DB-25 Female/Male, crossover</td>
<td>350</td>
</tr>
<tr>
<td>39</td>
<td>Cable 3 - Cyclades RJ-45 to DB-9 Female, crossover</td>
<td>351</td>
</tr>
<tr>
<td>40</td>
<td>Cable 4 - Cyclades RJ-45 to Cyclades RJ-45, straight-through</td>
<td>351</td>
</tr>
<tr>
<td>41</td>
<td>Cable 5 - Cyclades/Sun Netra Cable</td>
<td>352</td>
</tr>
<tr>
<td>42</td>
<td>Loop-Back Connector</td>
<td>352</td>
</tr>
<tr>
<td>43</td>
<td>Cyclades/Sun Netra Adapter</td>
<td>353</td>
</tr>
<tr>
<td>44</td>
<td>RJ-45 Female to DB-25 Male Adapter</td>
<td>353</td>
</tr>
<tr>
<td>45</td>
<td>RJ-45 Female to DB-25 Female Adapter</td>
<td>354</td>
</tr>
<tr>
<td>46</td>
<td>RJ-45 Female to DB-9 Female Adapter</td>
<td>354</td>
</tr>
<tr>
<td>47</td>
<td>Terminal Block Pins</td>
<td>356</td>
</tr>
<tr>
<td>48</td>
<td>Cable 1 for the TS110/100 - DB-9 Female to DB-9 Female, crossover half duplex</td>
<td>357</td>
</tr>
</tbody>
</table>
List of Figures

49. Cable 2 for the TS110/100 - DB-9 Female to DB-9 Female, crossover full duplex .... 357
50. Cable 2 for the TS110/100 - Terminal Block to Terminal Block, crossover half duplex 358
51. Cable 4 for the TS110/100 - Terminal Block to Terminal Block, crossover full duplex 358
52. Cable 5 for the TS110/100 - DB-9 Female to DB-25 Female, crossover ................. 359
53. Initial test ................................................................................................................. 393
54. Second screen, showing changed positions ............................................................... 394
55. User List default page ............................................................................................... 405
56. User Group List default page ................................................................................... 405
57. Access Limit List default page .................................................................................. 406
58. Serial Port Connection page .................................................................................... 417
59. Port Connection page ............................................................................................... 418
60. The Refresh button .................................................................................................... 418
61. SSH User Authentication Popup Window ................................................................. 419
62. Console Access Server diagram .............................................................................. 422
63. CAS diagram with various authentication methods ............................................... 423
64. Terminal Server diagram ......................................................................................... 425
65. Ports configured for Dial-in Access .......................................................................... 427
List of Figures

This page has been left intentionally blank.
## List of Tables

1. Hardware vs. Configuration Methods .................................................. 40
2. Applications Section ................................................................. 51
3. Configuration Section ............................................................... 52
4. Administration Section ............................................................... 53
5. Web User Management Section ..................................................... 53
6. Information Section ................................................................. 54
7. Master Cyclades Configuration (where it differs from the CAS standard) .... 134
8. Cyclades-TS configuration for Slave 1(where it differs from the CAS standard) 136
9. Cyclades-TS configuration for Slave 2(where it differs from the CAS standard) 137
10. General Options for the Help Wizard ............................................. 178
11. Help CLI Options - Synopsis 1 ....................................................... 180
12. Help CLI Options - Synopsis 2 ....................................................... 182
13. Help CLI Options - Synopsis 3 ....................................................... 183
14. Modbus parameters ................................................................. 186
15. IPDU Syslog messages format ....................................................... 295
16. AlterPath PM Regular Menu Options ........................................... 302
17. vi modes ................................................................. 329
18. vi navigation commands ............................................................ 329
19. vi file modification commands .................................................... 330
20. vi line mode commands ............................................................ 330
21. Process table ................................................................. 337
22. Cyclades-TS power requirements ............................................... 343
23. Cyclades-TS physical specifications ........................................... 344
24. Cyclades-TS safety specifications ............................................... 344
## List of Tables

25. Cyclades-TS environmental conditions ............................................. 344
26. Cables and their pin specifications .................................................. 347
27. Which cable to use ........................................................................... 348
28. TS110/100 Connector pin assignment ................................................. 355
29. Parameters Common to CAS, TS, & Dial-in Access ............................ 361
30. Mostly CAS-specific Parameters ....................................................... 372
31. TS Parameters .................................................................................. 383
32. Dial-in configuration Parameters ....................................................... 384
33. Files to be included in /etc/config_file and the program to use ............... 390
34. CPU LED Code Interpretation .......................................................... 400
35. Required information for the OpenSSL package ................................... 401
36. Windows XP + JREv1.4.0_01 or 02 .................................................... 415
Glossary

Authentication

Authentication is the process of identifying an individual, usually based on a username and password. In security systems, authentication is distinct from authorization, which is the process of giving individuals access to system objects based on their identity. Authentication merely ensures that the individual is who he or she claims to be, but says nothing about the access rights of the individual. (Source: www.webopedia.com)

Break Signal

A break signal is generated in an RS-232 serial line by keeping the line in zero for longer than a character time. Breaks at a serial console port are interpreted by Sun servers as a signal to suspend operation and switch to monitor mode.

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.

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.

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.

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.
Glossary

**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 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.

**KVM Switch (KVM)**
Keyboard-Video-Mouse Switches connect to the KVM ports of many computers and allow the network manager to access them from a single KVM station.

**Mainframe**
Large, monolithic computer system.

**MIBs**
Management Information Bases. SNMP-compliant devices, called agents, store data about themselves in MIBs and return this data to the SNMP requesters.

**Out-of-band network management**
In a computer network, when the management data is accessed through a network that is independent of the network used to carry data, this is called “out-of-band network management.”

**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.
Glossary

Profile
Usage setup of the Cyclades-TS either as a Console Access Server (CAS), a Terminal Server, or a Remote Access Server.

RADIUS
Protocol between an authentication server and an access server to authenticate users trying to connect to the network.

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.

RS-232
A set of standards for serial communication between electronic equipment defined by the Electronic Industries Association in 1969. Today, RS-232 is still widely used for low-speed data communication.

Secure Shell (SSH)
SSH has the same functionality as Telnet (see definition below), 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).

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-com-
Glossary

Pliant devices, called agents, store data about themselves in Management Information Bases (MIBs) and return this data to the SNMP requesters. (Source: Webopedia)

Telnet

Telnet is the standard set of protocols for terminal emulation between computers over a TCP/IP connection. It is 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. This enables you to control the server and communicate with other servers on the network. To start a Telnet session, you must log in to a server by entering a valid username and password. Telnet is a common way to remotely control Web servers. (from webopedia.com)

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

The UNIX name for the COM (Microsoft) port.

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.
Index

A
Access Method 86
Alarm 171
Authentication 114

B
Basic Wizard 78
Battery 33
Billing 429
Block Connector 358

C
Cable Length 346
CLI 40
Command Line Interface 40, 77
Configuration using a Web browser 47
Connectors 347
CronD 138
Custom Wizard 43

D
Data Buffers 140
Default Configuration Parameters 40
DHCP 155
DNS Server 42
Domain 42

E
Ethernet 41

F
Filters 159
Flash Memory Loss 389

G
Gateway 41
default 42
Generating Alarms 162

H
Hardware Specifications 343
Hardware Test 392
HyperTerminal 41

I
Industrial automation 185
IP Address 42

K
Kermit 41

L
Linux File Structure 326
Linux-PAM 272

M
Minicom 41
MODBUS 185
# Index

Modbus 185

**N**
- Netmask 42
- NTP 187

**P**
- Passwords 325
- Port Test 392

**R**
- Radius authentication 427
- Routing Table 331
- RS-232 Standard 345
- RS-485 Standard 355

**S**
- Secure Shell Session 332

Sendmail 171
- Sendsms 171
- serial ports 20
- Smnptrap 171
- Syslog-n 239
- System Requirements 39

**T**
- Terminal Appearance 255
- Time Zone 264

**U**
- Upgrades 387
- Using 84
- Using the Wizard through your Browser 84

**W**
- Wizard 42