
Cyclades-TS User Guide

Version 1.3.4 Revision 3.1

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

©Cyclades Corporation, 2002

Cyclades-TS Version 1.3.4 Revision 3.1 User Guide

November 2002

Copyright © Cyclades Corporation, 2002

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 v1.3.4. 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, and Cyclades-TS100 are registered trademark of Cyclades Corporation. Microsoft, Windows 95, 98, XP, ME, NT, and 2K are trademarks of Microsoft Corporation. UNIX is a trademark of UNIX System Laboratories, Inc. Linux is a registered trademark of Linus Torvald.

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.

Product Version 1.3.4 Revision 3.1
Document Number 1.3.4-Draft 13

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	13
Glossary Entries	13
Note Box Icons	14
Quick Steps	15

Chapter 1 - Introduction and Overview

Introducing Cyclades	17
The Cyclades-TS	17
Console Access Server	18
What's in the box	20
Powering the TS100	25
Power Supply Installation	26
Safety Instructions	27
Replacing the Battery	29
FCC Warning Statement	30

Chapter 2 - Installation and Configuration

Introduction	31
System Requirements	31
Default Configuration Parameters	32
Pre-Install Checklist	33
Task List	34
The Wizard	34
Quick Start	36
Configuration using a Console	36
Configuration using a Web browser	39
Configuration using Telnet	46
The Installation and Configuration Process	49

Table of Contents

Task 1: Connect the Cyclades-TS to the Network and other Devices . . .	49
Task 2: Configure the COM Port Connection and Log In	52
Task 3: Modify the System Files	53
Task 4: Edit the pslave.conf file	57
Task 5: Activate the changes	59
Task 6: Test the configuration	59
Task 7: Save the changes	60
Task 8: Reboot the Cyclades-TS	60
Special Configuration for the Cyclades-TS100	61
TS100-specific background information	61
Configuring the Cyclades-TS100 for the first time	62

Chapter 3 - Additional Features

Introduction	63
Configuration Wizard - Basic Wizard	64
Using the Wizard through your Browser	69
Access Method	71
Configuration for CAS	71
Configuration for TS	85
Configuration for Dial-in Access	91
Authentication	95
Parameters Involved and Passed Values	95
Configuration for CAS, TS, and Dial-in Access	97
Clustering	104
Parameters Involved and Passed Values	105
Centralized Management - the Include File	108
CronD	112
Parameters Involved and Passed Values	112
Configuration for CAS, TS, and Dial-in Access	113
Browser Method	113
Data Buffering	114
Introduction	114
Linear vs. Circular Buffering	115
Parameters Involved and Passed Values	116
Configuration for CAS	118
DHCP	125
Parameter Involved and Passed Values	125
Configuration for CAS, TS, and Dial-in Access	127

Table of Contents

Filters	129
Description	129
Configuration for CAS, TS, and Dial-in Access	130
Generating Alarms	131
Port Slave Parameters Involved with Generating Alarms	131
vi Method	132
Browser Method	132
Wizard Method	133
Syslog-ng Configuration to use with Alarm Feature	136
Alarm, Sendmail, Sendsms and Snmptrap	138
Help	145
Help Wizard Information	145
Help Command Line Interface Information	146
Modbus	148
NTP	152
Parameters Involved and Passed Values	152
Configuration for CAS, TS, and Dial-in Access	153
Ports Configured for Dial-in Access	154
Ports Configured as Terminal Servers	156
TS Setup Scenario	157
TS Setup Wizard	158
Serial Settings	161
Parameters Involved and Passed Values	161
Configuration for CAS	163
Configuration for TS	170
Configuration for Dial-in Access	174
Session Sniffing	174
Versions 1.3.2 and earlier	174
Versions 1.3.3 and later	175
Parameters Involved and Passed Values	177
Configuration for CAS	178
Wizard Method	179
SNMP	183
Configuration for CAS, TS, and Dial-in Access	185
Syslog	185
Port Slave Parameters Involved with syslog-ng	186
Configuration for CAS, TS, and Dial-in Access	187
Wizard Method	188
The Syslog Functions	191

Table of Contents

Terminal Appearance	206
Parameters Involved and Passed Values.	206
Configuration for CAS, TS, and Dial-in Access.	206
Wizard Method	207
Time Zone.	211
How to set Date and Time	212

Appendix A - New User Background Information

Users and Passwords.	213
Linux File Structure	213
Basic File Manipulation Commands	214
The vi Editor	215
The Routing Table	217
Secure Shell Session	218
The Process Table.	222
TS Menu Script	223

Appendix B - Cabling, Hardware, and Electrical Specifications

General Hardware Specifications	226
The RS-232 Standard	228
Cable Length.	229
Connectors	229
Straight-Through vs. Crossover Cables	230
Which cable should be used?	231
Cable Diagrams	232
TS100-only cabling information	238
The RS-485 Standard	238
TS100 Connectors	238
Cable diagrams	240

Appendix C - The pslave Configuration File

Introduction	243
Configuration Parameters	243
CAS Parameters	243
TS Parameters	258
Dial-in Access Parameters	259

Table of Contents

Appendix D - Linux-PAM

Introduction	262
The Linux-PAM Configuration File	264
Configuration File Syntax	264
Newest Syntax	267
Module Path	269
Arguments	271
Directory-based Configuration	273
Default Policy	273
Reference	279

Appendix E - Customization and the Cyclades Developer Kit

Introduction	280
The Customization Process	281
The Cyclades Development Kit	281

Appendix F - Software Upgrades and Troubleshooting

Upgrades	282
The Upgrade Process	282
Troubleshooting	284
Flash Memory Loss	284
Hardware Test	287
Port Test	287
Port Conversation	288
Test Signals Manually	288
Single User Mode	289
Troubleshooting the Web Configuration Manager	291
What to do when the initial Web page does not appear	291
How to restore the Default Configuration of the Web Configuration Manager	291
Using a different speed for the Serial Console	292
CPU LED	293

Appendix G - Certificate for HTTP Security

Introduction	295
Procedure	295

Table of Contents

Appendix H - How to Connect to Serial Ports from the Browser

Introduction	298
Tested Environment	298
On Windows	299
From Internet Explorer	299
From Netscape or Mozilla	299
On Linux	300
From Netscape or Mozilla	300
Step-by-Step Process	300

List of Wiz Application Parameters

Basic Parameters (wiz)	303
Authentication Parameters (wiz --auth)	303
Terminal Appearance Parameters (wiz --tl)	304
Alarm Parameter (wiz --al)	304
Data Buffering Parameters (wiz --db)	304
Sniffing Parameters (wiz --snf)	305
Syslog Parameters (wiz --sl)	305
Terminal Server Profile Other Parameters (wiz --tso)	305
Access Method Parameters (wiz --ac <type>)	306
Serial Settings Parameters (wiz --sset <type>)	307

List of Figures	308
---------------------------	-----

List of Tables	311
--------------------------	-----

Glossary	313
--------------------	-----

Index	317
-----------------	-----

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 and Configuration](#) 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.
- [Chapter 3 - Additional Features](#) is dedicated to users wanting to explore all available features of the Cyclades-TS. It provides configuration instructions for syslog, data buffers, authentication, filters, DHCP, NTP, SNMP, clustering, and sniffing.
- [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 - Linux-PAM](#) enables the local system administrator to choose how to authenticate users.
- [Appendix E - Customization and the Cyclades Developer Kit](#) provides instruction for those who wish to create their own applications.
- [Appendix F - Software Upgrades and Troubleshooting](#) includes solutions and test procedures for typical problems.
- [Appendix G - Certificate for HTTP Security](#) provides configuration information that will enable you to obtain a Signed Digital Certificate.
- [Appendix H - How to Connect to Serial Ports from the Browser](#) enables this process, based on how the serial port is configured.

Preface

Additional Documentation and Help

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

- The Cyclades Console Port Management Guide
- The Cyclades Product Catalog

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

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

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.

Preface

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 . . .

Preface

This page has been left intentionally blank.

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 plain-text 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

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 and Configuration](#) 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](#).

Console Access Server

An example of a CAS environment is shown in [Figure 1: Console Access Server diagram](#). This configuration example has local authentication, an Ethernet interface provided by a router, and serially-connected workstations.

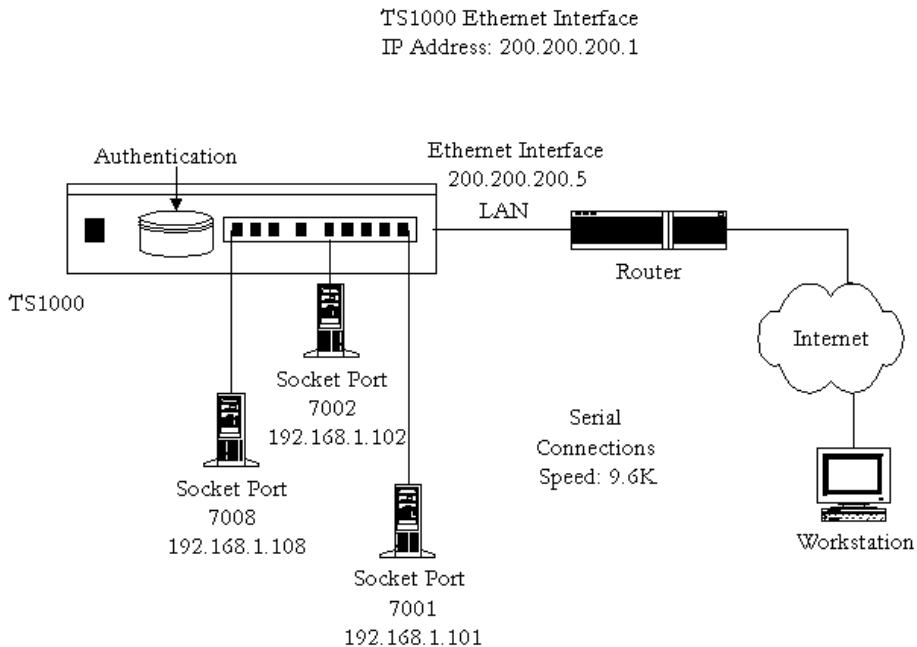


Figure 1: Console Access Server diagram

Introduction and Overview

The following diagram, [Figure 2: CAS diagram with various authentication methods](#), shows additional scenarios for the Cyclades-TS: both remote and local authentication, data buffering, and remote access.

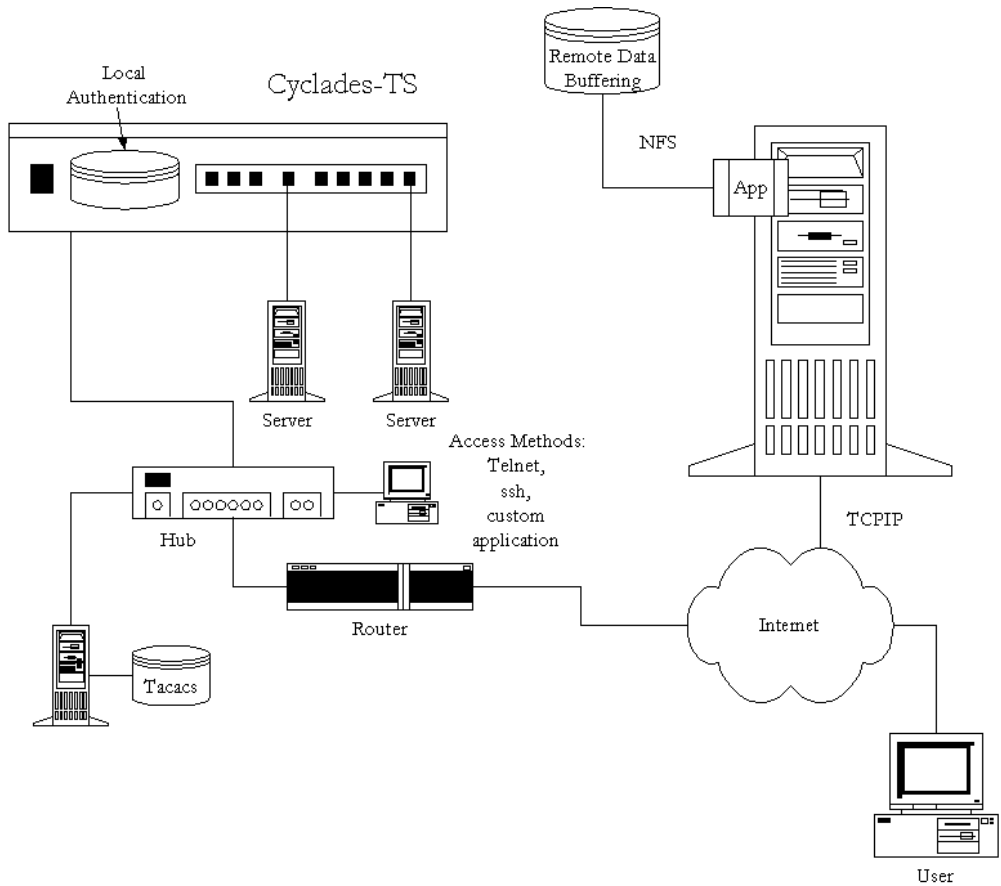


Figure 2: CAS diagram with various authentication methods

Introduction and Overview

What's in the box

There are several models of the Cyclades-TS with differing numbers of serial ports. The following figures show the main units and accessories included in each package. The RJ-45 straight-through cable is the main cable that you will use. After configuration, the RJ-45 cable and its adapter can be used to connect to the server. Four adapters are included: two RJ-45 to DB-9 (male and female) and two RJ-45 to DB-25 (male and female). Select the adapter appropriate to your COM port. A power cable, a modem cable, manual and mounting kit are also included in the box. The Sun Netra Crossover cable is included with the TS3000, TS2000, TS1000, TS800 and TS400. The loop-back connector is provided for convenience in case hardware tests are necessary.

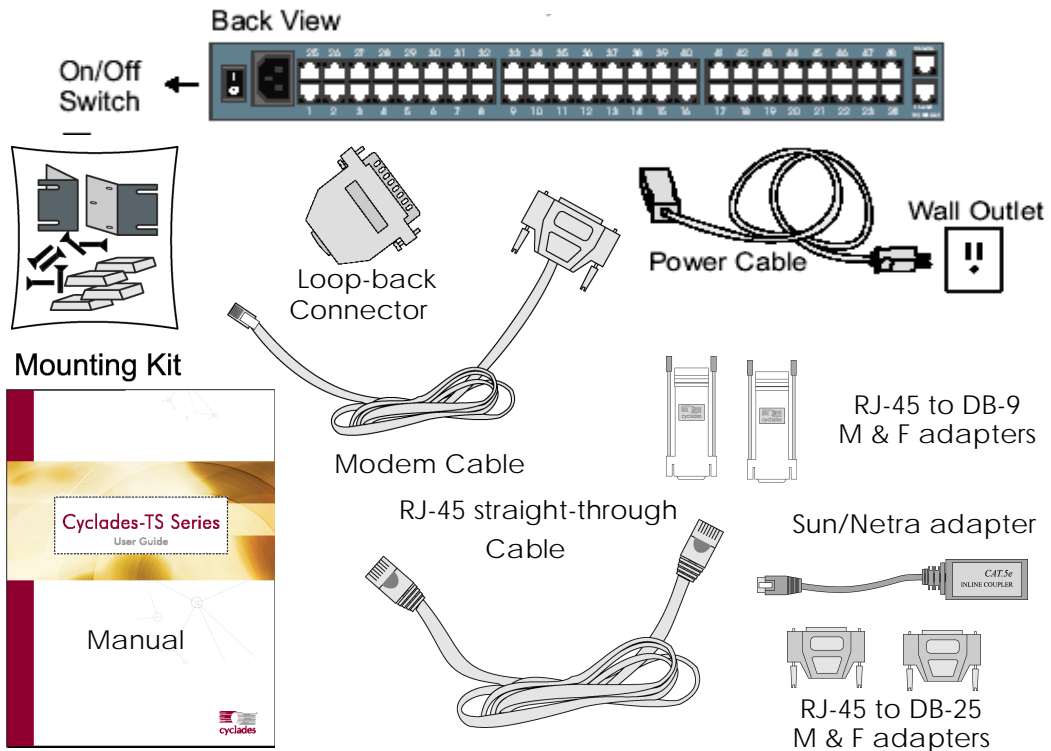


Figure 3: The Cyclades-TS3000 and cables

Introduction and Overview

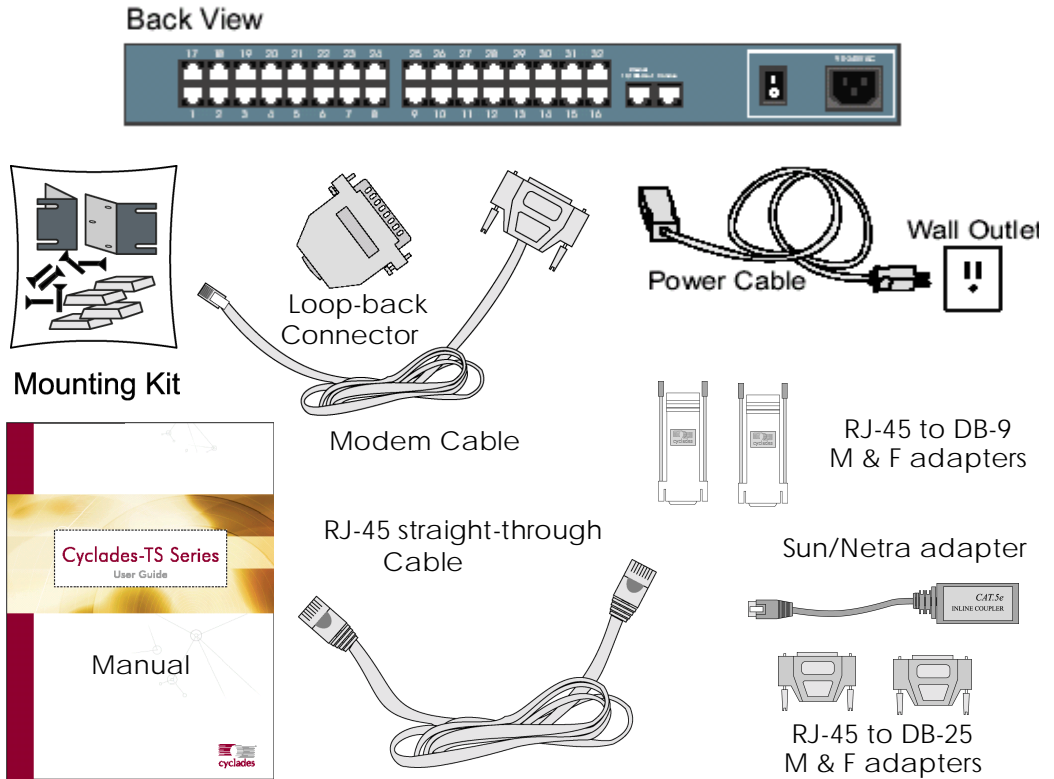


Figure 4: The Cyclades-TS2000 and cables

Introduction and Overview

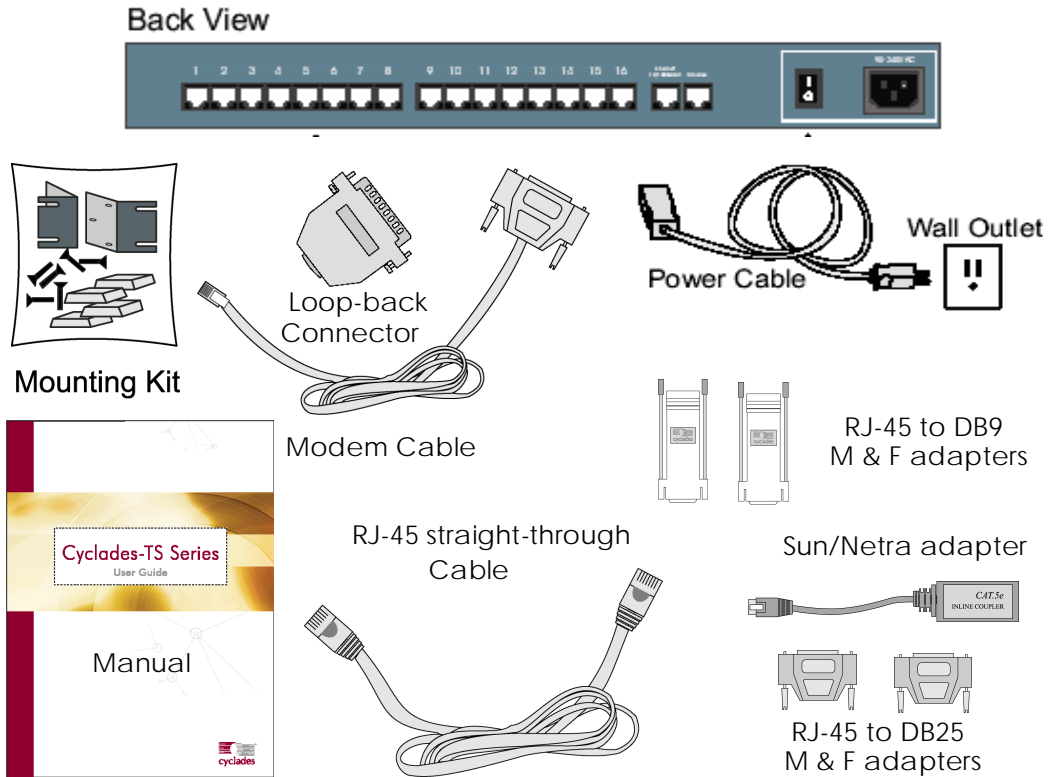


Figure 5: The Cyclades-TS1000 and cables

Introduction and Overview

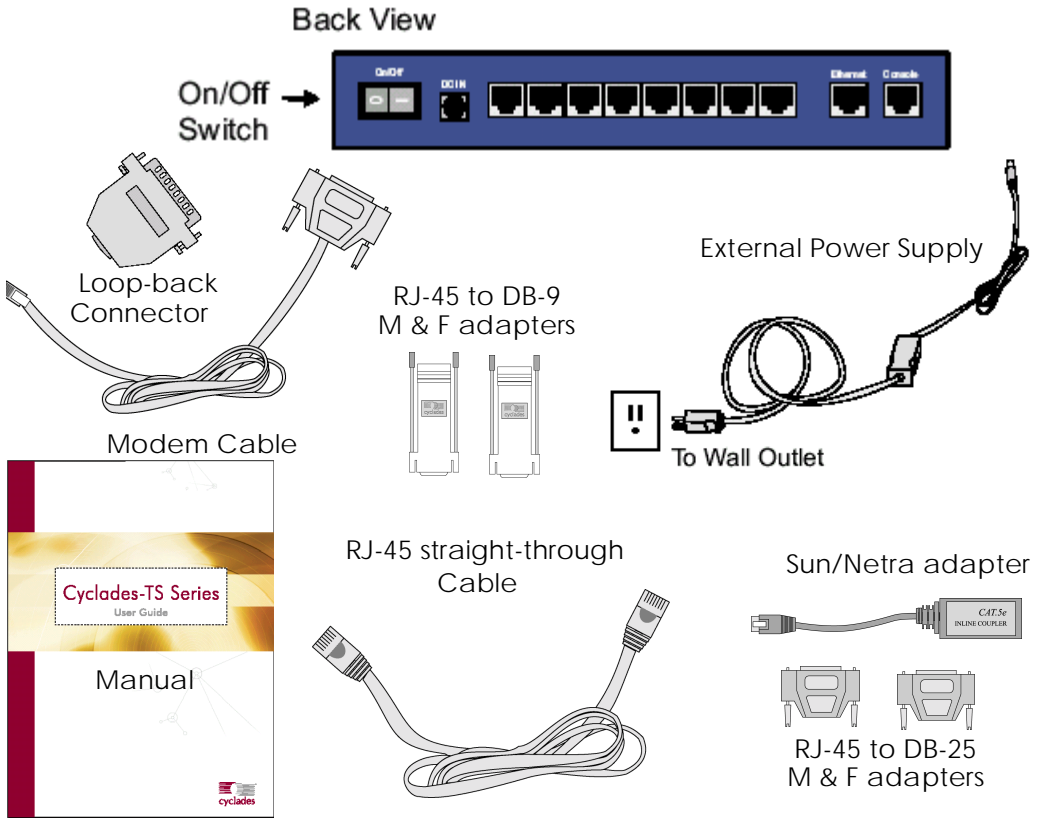


Figure 6: The Cyclades-TS800 and cables

Introduction and Overview

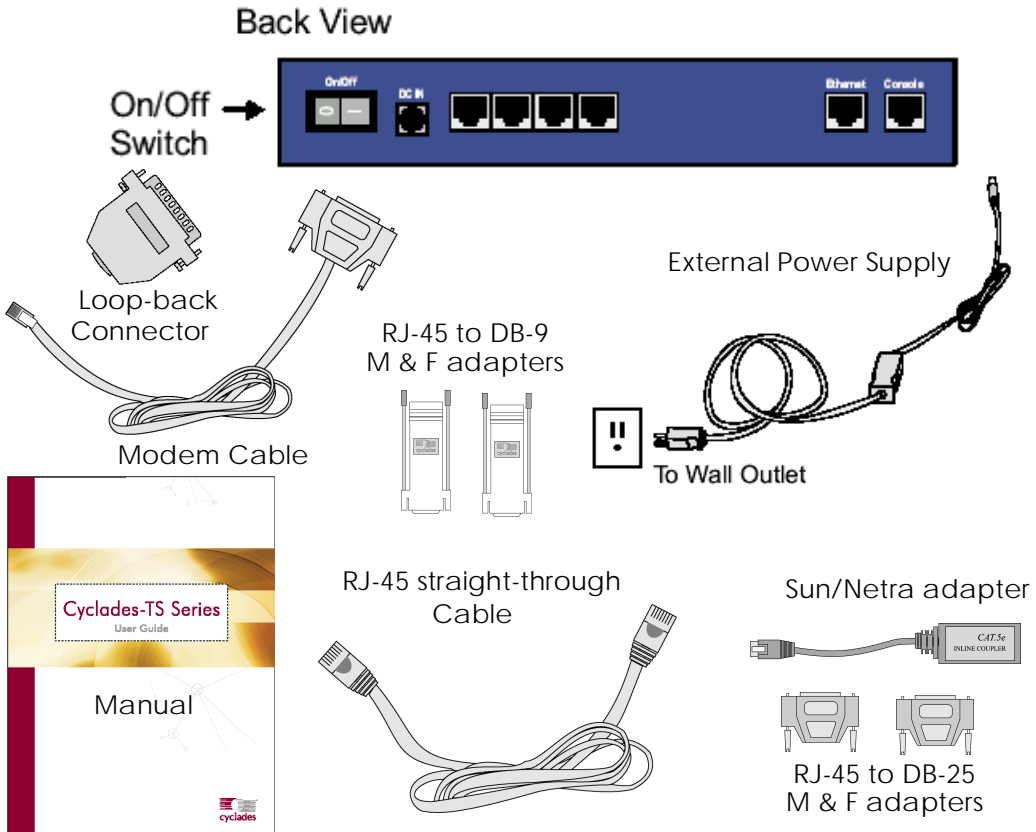


Figure 7: The Cyclades-TS400 and cables

Introduction and Overview

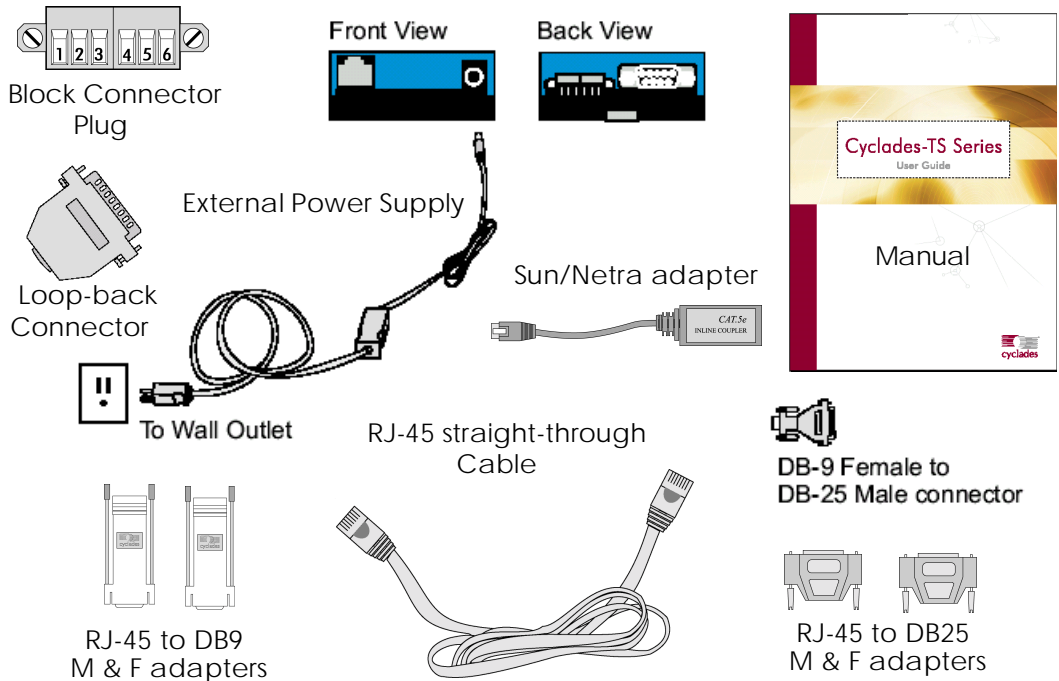


Figure 8: The Cyclades-TS100 and cables

Powering the TS100

There are three ways to supply power to TS100:

1. **External AC Desktop Power Supply: Universal AC Input (100-240VAC) / 5VDC Output.** This power supply is shipped with the standard TS100 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)

Introduction and Overview

3. P.O.E. (Power Over Ethernet)

The power is supplied through the Ethernet cable. When this option is selected, the TS100 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. TS100 supports both standards.

Power Supply Installation

External Desktop AC Power Supply

Step 1: Connect one end of the power cable to the TS100 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+.



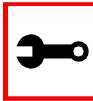
Notes:

- There is a label on the TS100 unit showing the nominal DC input voltage.
- The external desktop AC Power Supply (Universal AC input / 5VDC output) is not shipped with the TS100 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 TS100 just won't work. It does not cause any damage to the unit.

Introduction and Overview

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 TS100 as standard accessory.

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.

Introduction and Overview



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 TS100, 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.



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.



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.

Introduction and Overview



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

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:

- 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 TS100 does not have the battery, so the date and time must be kept up-to-date by ntpclient. If you have to repeatedly reset time and date information after turning on your Cyclades-TS, replace the battery.



DANGER! A new battery can explode if it is incorrectly installed. Replace the 3-Volt CR2032 battery only with the same or equivalent type recommended by the battery manufacturer. Discard used batteries according to the battery manufacturer's instructions.

Introduction and Overview

FCC Warning Statement

The Cyclades-TS has been tested and found to comply with the limits for Class A digital devices, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the Installation & Service Manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user is required to correct the problem at his or her own expense.

Notice about FCC compliance for 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.

Canadian DOC Notice

The *Cyclades-TS* does not exceed the Class A limits for radio noise emissions from digital apparatus set out in the Radio Interference Regulations of the Canadian Department of Communications.

Le Cyclades-TS n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de la classe A prescrites dans le règlement sur le brouillage radioélectrique édicté par le Ministère des Communications du Canada.

Chapter 2 - Installation and Configuration

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

Chapter 2 - Installation and Configuration

The following table shows the different hardware required for various configuration methods:

Table 1: Hardware vs. Configuration Methods

Hardware	Configuration Method
Console, Console Cable (constructed from RJ-45 straight-through cable + adapter)	vi, Wizard, or CLI
Workstation, Hub, Ethernet Cables	vi, Wizard, CLI, or browser

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 Net-mask of 255.255.255.0)
- CAS configuration
- socket_server in all ports (access method is telnet)
- 9600 bps, 8N1
- No Authentication

Chapter 2 - Installation and Configuration

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:
PC or terminal,
Cyclades-TS,
NameServer, and
Gateway*

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. 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.

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 and Configuration

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

Chapter 2 - Installation and Configuration

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](#)
- [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-TS100, there are special requirements and instructions. Be sure to read [Special Configuration for the Cyclades-TS100](#) at the end of this chapter.

Chapter 2 - Installation and Configuration

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.

Chapter 2 - Installation and Configuration

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.

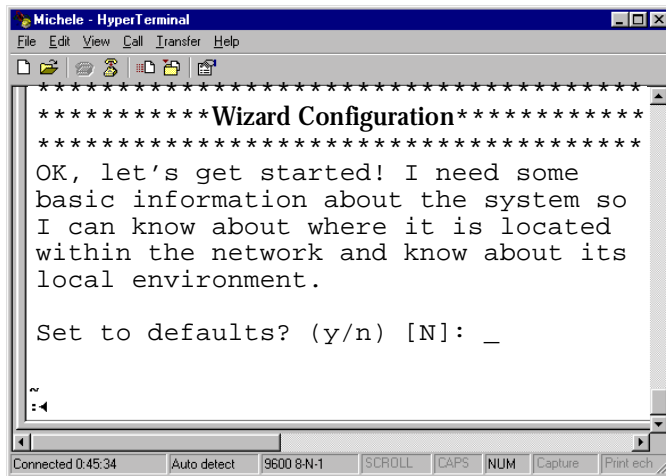


Figure 9: The initial wizard configuration screen - console configuration method

You will want to configure the following settings:

- Hostname
- DHCP enabled/disabled
- System IP (if DHCP is disabled)
- Domain Name
- Primary DNS Server
- Gateway IP
- Network Mask(if DHCP is disabled)

Chapter 2 - Installation and Configuration

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

Your current configuration parameters are:

Hostname : CAS

DHCP : Enabled

Domain name : cyclades.com

Primary DNS Server : 197.168.160.200

Gateway : 192.168.160.10

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 and Configuration

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.

Chapter 2 - Installation and Configuration

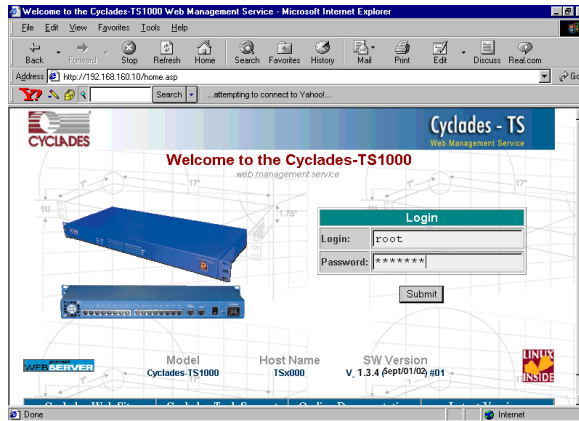


Figure 10: Login page of Web Configuration Manager

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:

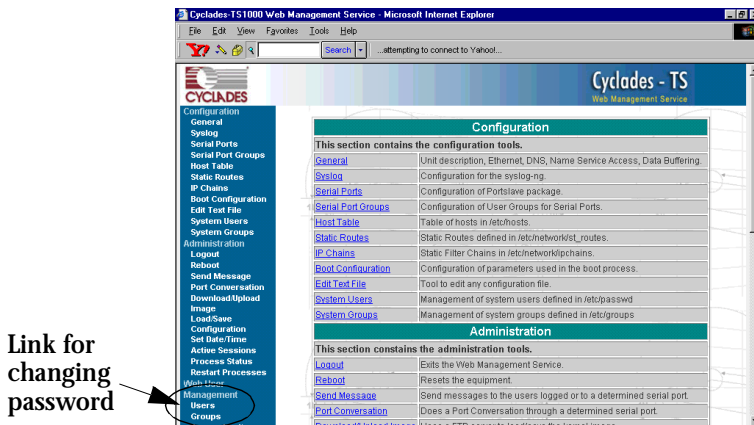


Figure 11: Configuration & Administration Menu page

Chapter 2 - Installation and Configuration

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 2: Configuration Section](#) through [Table 5: 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 [How to change the Password of Web Users](#).

Step 6: Click on the General link.

Description	
Hostname:	TS000
Console Banner:	Cyclades-TS
Ethernet port	
Primary IP Address:	192.168.160.10
Network Mask:	255.255.255.0
Secondary IP Address:	
Network Mask:	
Common Configuration File Name:	
DHCP Client:	<input checked="" type="radio"/> inactive <input type="radio"/> active <input type="radio"/> act & restores last assigned
MTU:	1500
DNS Service	
Primary DNS Server:	

Figure 12: General page

Step 7: Configure parameters presented in the fields.

Step 8: Click on the Submit button.

Step 9: Click Administration > Restart Processes > signal_ras hup.

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 10: Click the link Administration > Load/Save Configuration.

Chapter 2 - Installation and Configuration

Step 11: 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
```



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 your browser, use the vi editor from the console, or use CLI, if appropriate.

How to change the Password of Web Users

Step 1: Click on the link Web User Management > Users.

Step 2: Select the user *root*.

Step 3: Click on the Change Password button.

Step 4: Type the new password twice.

Step 5: Submit the request.

The next page will require a new login.

Step 6: Type *root* and the new password.

Step 7: Click on the link Web User Management > Load/Save Configuration.

Step 8: Click the Save Configuration button.

Chapter 2 - Installation and Configuration

Table 2: Configuration Section

Link Name	Description of Page Contents
<i>General</i>	Description, Ethernet, DNS, Name Service Access, Data Buffering
<i>Syslog</i>	Configuration for the syslog-ng
<i>Serial Ports</i>	Configuration for the Portslave package
<i>Connect to Serial Ports</i>	Telnet/SSH connection to Portslave. (See Note Box below.)
<i>Serial Port Groups</i>	User Groups in Serial Ports Configuration
<i>Host Table</i>	Table of hosts in /etc/hosts
<i>Static Routes</i>	Static routes defined in /etc/network/st_routes
<i>IP Chains Filter</i>	Shows IP Chains entries.
<i>Boot Configuration</i>	Configuration of parameters used in the boot process
<i>Edit Text File</i>	Tool to read and edit a configuration file
<i>System Users</i>	Management of system users defined in /etc/password
<i>System Groups</i>	Management of system groups defined in /etc/groups

Chapter 2 - Installation and Configuration

Table 3: Web User Management Section

Link Name	Description of Page Contents
<i>Users</i>	List of users allowed to access the Web server
<i>Groups</i>	List of possible access groups
<i>Access Limits</i>	List of access limits for specific URLs
<i>Load/Save Configuration</i>	Load/Save Web user configuration in /etc/websum.conf

Table 4: Administration Section

Link Name	Description of Page Contents
<i>Logout</i>	Exits the Web Manager
<i>Reboot</i>	Resets the equipment
<i>Port Conversation</i>	Initiates a port conversation through a serial port
<i>Download/Upload Image</i>	Uses an FTP server to load and save a kernel image
<i>Load/Save Configuration</i>	Uses flash memory or an FTP server to load or save the TS's configuration
<i>Set Date/Time</i>	Set the TS's date and time
<i>Active Sessions</i>	Shows the active sessions
<i>Process Status</i>	Shows the running processes and allows the administrator to kill them
<i>Restart Processes</i>	Allows the administrator to start or stop some processes
<i>PCMCIA</i>	Allows the administrator to insert and eject PCMCIA cards

Chapter 2 - Installation and Configuration

Table 5: Information Section

Link Name	Description of Page Contents
<i>Interface Statistics</i>	Shows statistics for all active interfaces
<i>DHCP client</i>	Shows the DHCP client information
<i>Serial Ports</i>	Shows the status of all serial ports
<i>Routing Table</i>	Shows the routing table and allows the administrator to add or delete routes
<i>ARP Cache</i>	Shows the ARP cache
<i>IP Chains</i>	Shows IP Chains entries
<i>IP Rules</i>	Shows Firewall, NAT, and IP Accounting rules
<i>IP Statistics</i>	Shows IP protocol statistics
<i>ICMP Statistics</i>	Shows ICMP protocol statistics
<i>TCP Statistics</i>	Shows TCP protocol statistics
<i>UDP Statistics</i>	Shows UDP protocol statistics
<i>RAM Disk Usage</i>	Shows the TS file system
<i>System Information</i>	Shows information about the kernel, time, CPU, and memory

Chapter 2 - Installation and Configuration

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.

Chapter 2 - Installation and Configuration

Step 5: Type *wiz* and press Enter.

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

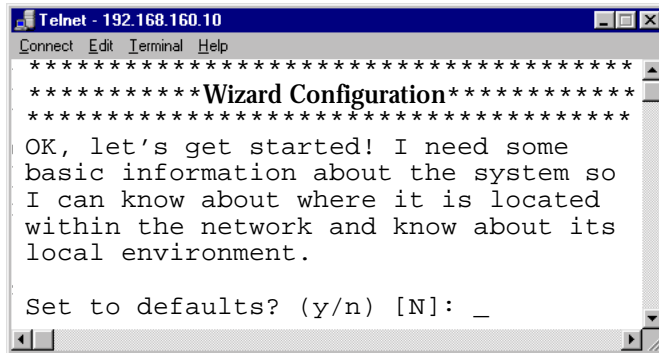


Figure 13: The initial wizard configuration screen - telnet configuration method

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

Your current configuration parameters are:

Hostname : CAS

DHCP: disabled

System IP : 192.168.160.10

Domain name : cyclades.com

Primary DNS Server : 197.168.160.200

Gateway : 192.168.160.10

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.

Chapter 2 - Installation and Configuration

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 use a browser or CLI (if appropriate). For additional configuration, see [Chapter 3 - Additional Features](#) in this guide.

Chapter 2 - Installation and Configuration

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 hup` (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 and Configuration



Tip. We strongly recommend to use 9600 bps console speed. In case you need to use another speed please check [Appendix F - 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. 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).

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.

Chapter 2 - Installation and Configuration



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 TS100, 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/hpte/download.html>

Chapter 2 - Installation and Configuration

Task 2: Configure the COM Port Connection and Log In

Step 1: Select available COM port.

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

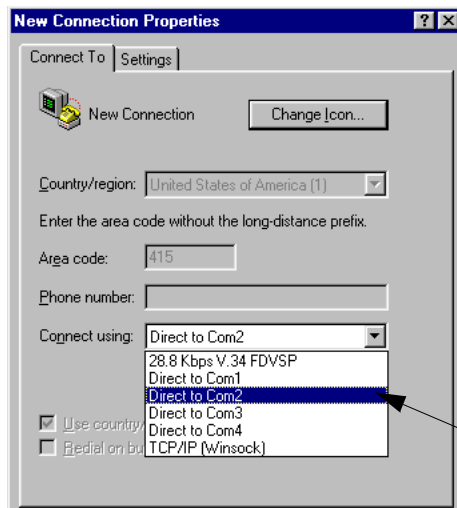


Figure 14: Choose a free COM port

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).

Chapter 2 - Installation and Configuration

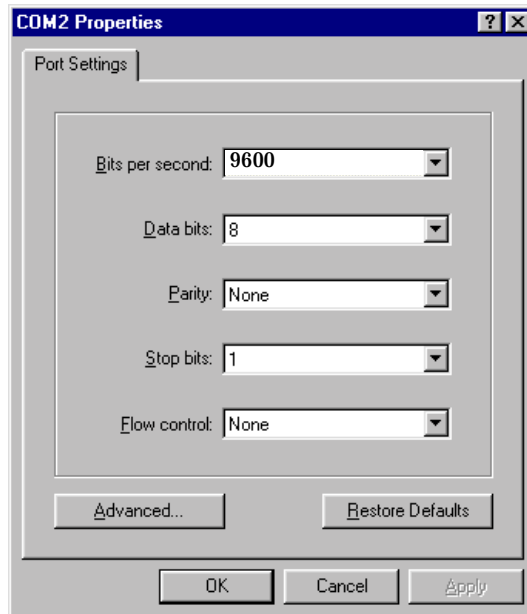


Figure 15: Port Settings

Step 3: Power on the Cyclades-TS.

Step 4: Click OK on the Properties window.

You will see the Cyclades 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 and /etc/inittab (Cyclades-TS100 only)
```

Chapter 2 - Installation and Configuration



Important! If you have the Cyclades-TS100 you will be modifying an additional file: `/etc/inittab`. See [Configuring the Cyclades-TS100 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.)

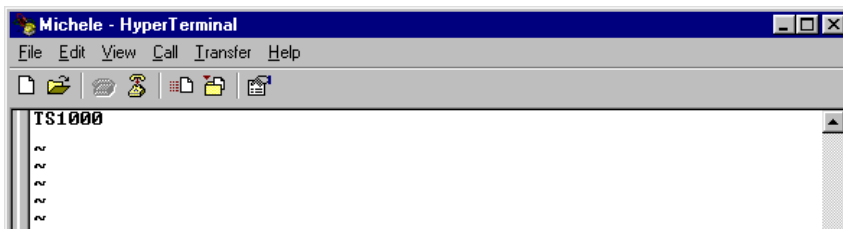


Figure 16: The `/etc/hostname` file with hostname typed in

Chapter 2 - Installation and Configuration

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.

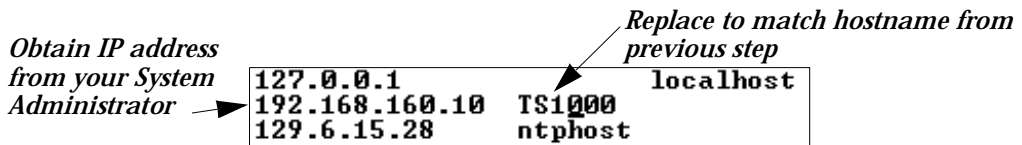


Figure 17: Contents of the /etc/hosts file

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:

```
domain      mycompany.com
nameserver  200.200.200.2
```

Step 6: Modify /etc/network/st_routes.

The fourth file defines static routes. In the console server example in [Figure 1: 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:

Chapter 2 - Installation and Configuration

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

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

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

```
# adduser boo
```

Step C: Edit the file `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`.

Step D: Edit the `passwd` file.

Replace the password in all password fields with an “x”. The root’s line will look like this:

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



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`.”

Chapter 2 - Installation and Configuration

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`



Tip. You can do a find for each of these parameters in vi, once you open this file by typing `/ <your string>` to search the file downward for the string specified after the `/`.

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.

Chapter 2 - Installation and Configuration

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

all.authtype

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:

- *local* (authentication is performed using the `/etc/passwd` file)
- *radius* (authentication is performed using a Radius authentication server)
- *TacacsPlus* (authentication is performed using a TacacsPlus authentication server)
- *local/radius* (authentication is performed locally first, switching to Radius if unsuccessful)
- *none* (no authentication)
- *radius/local* (the opposite of the previous option)
- *RadiusDownLocal* (local authentication is tried only when the Radius server is down)
- *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/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)

An example value would be:

radius

Chapter 2 - Installation and Configuration

- 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 F - Software Upgrades and Troubleshooting](#).

Chapter 2 - Installation and Configuration

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 theTS 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 F - Software Upgrades and Troubleshooting](#).

Task 7: Save the changes

Execute the following command in HyperTerminal to save the configuration:

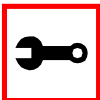
```
saveconf
```

Task 8: Reboot the Cyclades-TS

After rebooting, the initial configuration is complete.



Note: `saveconf` is equivalent to `tar -czf /proc/flash/script -T /etc/config_files` in standard Linux (`saveconf` must be used because `tar` on theTS does not support the `z` flag).



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 and Configuration

Special Configuration for the Cyclades-TS100

TS100-specific background information

Since there are two physical interfaces available in the Cyclades-TS100--RS-232 and RS-485--this model requires the configuration of the parameter described below.

*all.media or**
s1.media

(*see note box
below)

For the TS100 only.

- rs232 (RS-232 interface and DB-9 connector),
- rs485_half_terminator (RS-485 interface, half duplex communication with two wires, DB-9 or block connector. The TS100 terminates the network),
- rs422 (RS-485 interface, full duplex communication with four wires, DB-9 or block connector. The TS100 terminates the network), or
- rs485_half (RS485 interface, half duplex communication with two wires, DB-9 or block connector. The TS100 is in the middle of the network.)



Note: *all.** parameters are used to set default parameters for all ports and *s#.** parameters change the default parameters for individual ports. As the TS100 has only one port, either *s1** or *all.** can be used interchangeably.

Chapter 2 - Installation and Configuration

Configuring the Cyclades-TS100 for the first time

The next step is to update the system with the modified data in the files above. Make sure the file named `/etc/config_files` contains the names of all files that should be saved to flash.

The Cyclades-TS100 does not have a dedicated console port. Therefore, after configuring the serial port, perform the following steps:

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
```

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 TS100, the initial configuration is complete.

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](#)
- [Clustering](#)
- [CronD](#)
- [Data Buffering](#)
- [DHCP](#)
- [Filters](#)
- [Generating Alarms](#)
- [Help](#)
- [NTP](#)
- [Ports Configured for Dial-in Access](#)
- [Ports Configured as Terminal Servers](#)
- [Serial Settings](#)
- [Session Sniffing](#)
- [SNMP](#)
- [Syslog](#)
- [Terminal Appearance](#)
- [Time Zone](#)

Chapter 3 - Additional Features

Configuration Wizard - Basic Wizard

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:

4. /etc/hostname
5. /etc/hosts
6. /etc/resolv.conf
7. /etc/network/st_routes
8. /etc/network/ifcfg_eth0
9. /etc/portslave/pslave.conf

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 prompt.

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

Step 2: 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.

Chapter 3 - Additional Features



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, 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 number if you do not wish to configure the value.

Step 3: 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]:
```

Step 4: Type *y*, *n*, or press Enter to enable or disable DHCP client.

Type *y* 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* or press Enter to manually assign an IP address.

```
Do you want to use dhcp to automatically assign an IP for  
your system (Y)es or (N)o [N]:
```



Note: Typing *y* omits Steps 5 and Step 9.

Chapter 3 - Additional Features

Step 5: 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 6: Enter Domain name and then press Enter.

Domain name locates or identifies your organization within the Internet.

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

Step 7: 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 8: 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.

```
Gateway IP[eth0]: 192.168.160.10
```

Step 9: 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 10: Review configuration parameters.

You will now have the parameters you just configured displayed back to you. If you entered *y* in Step 4:

```
Your current configuration parameters are:
```


Chapter 3 - Additional Features

```
Hostname: CAS
DHCP: Enabled
Domain Name: cyclades.com
Primary DNS Server: 197.168.160.200
Gateway: 192.168.160.10
Are all these parameters correct (Y)es or (N)o [N]:
```

If you entered *n* in Step 4:

Your current configuration parameters are:

```
Hostname: CAS
DHCP: disabled
System IP: 192.168.160.10
Domain Name: cyclades.com
Primary DNS Server: 192.168.160.200
Gateway: 192.168.160.10
Network Mask: 255.255.255.0
Are all these parameters correct (Y)es or (N)o [N]:
```

Step 11: Type *y*, or *n*, or press Enter.

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

If *n* is entered, this is displayed:

```
Type 'c' to go back and CORRECT the current configuration
parameters or 'q' to QUIT:
```

Step 12: If you typed *n* in Step 11, type *c* or *q*.

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

Chapter 3 - Additional Features

Step 13: If you typed *y* in Step 11, choose whether to activate your configurations.

```
*****
***** 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 configura-
tions, 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] :
```

Step 14: 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 *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

Chapter 3 - Additional Features

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 15: 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 18: 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 19: Port Selection page](#)), clicking Submit, and then selecting either the CAS, TS, or RAS profile buttons on the subsequent Serial Port Configuration Page ([Figure 20: 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:

Chapter 3 - Additional Features

For CAS:

- Port Speed
- First RADIUS/TacacsPlus Authentication Server
- 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)

Chapter 3 - Additional Features

Access Method

Access method is how a user accesses a server connected with one of the serial ports on the Cyclades-TS. You can access through telnet, SSH, raw data, or modbus. *The first three methods are CAS-related.* Modbus is dedicated towards industrial automation. Access method also refers to users' access to the serial port, based on common users and administrative users. Accessing the Cyclades-TS with a browser allows for both telnet and ssh methods.

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.
- all.sttyCmd* The stty command which can be issued to configure the serial port.
- 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*.

Chapter 3 - Additional Features

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 TS.

In the address field of your browser type:

<Console Access Server's IP address>

Step 2: Log in.

Log in as root, pwd is tslinux. This will take you to the Configuration and Administration page.

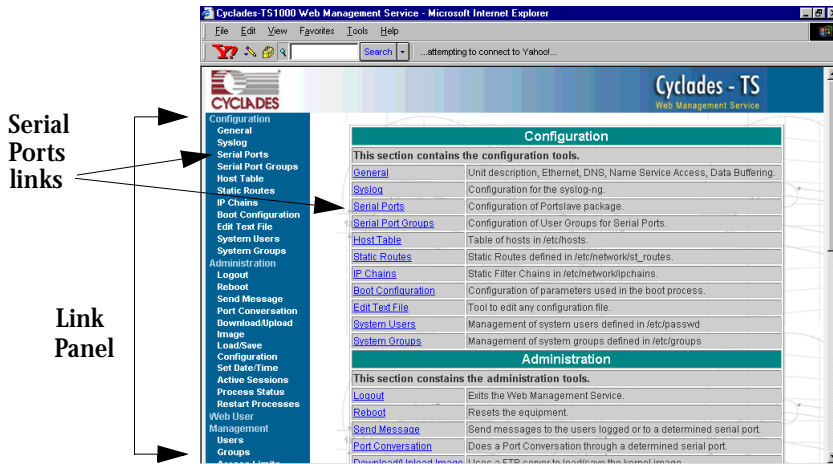


Figure 18: Configuration and Administration page

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

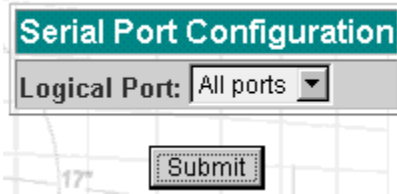


Figure 19: Port Selection page

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.

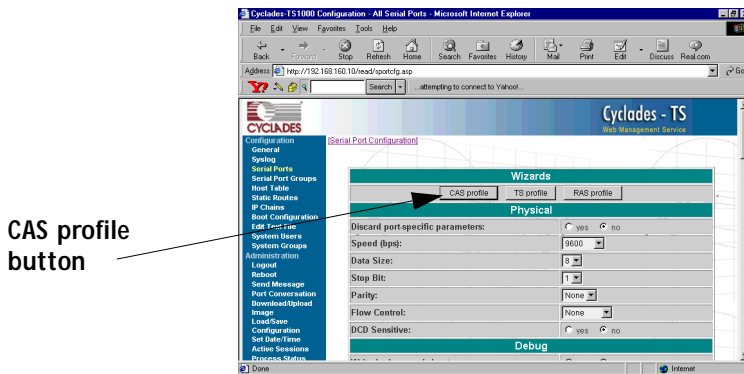


Figure 20: Serial Port Configuration page

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.

Chapter 3 - Additional Features

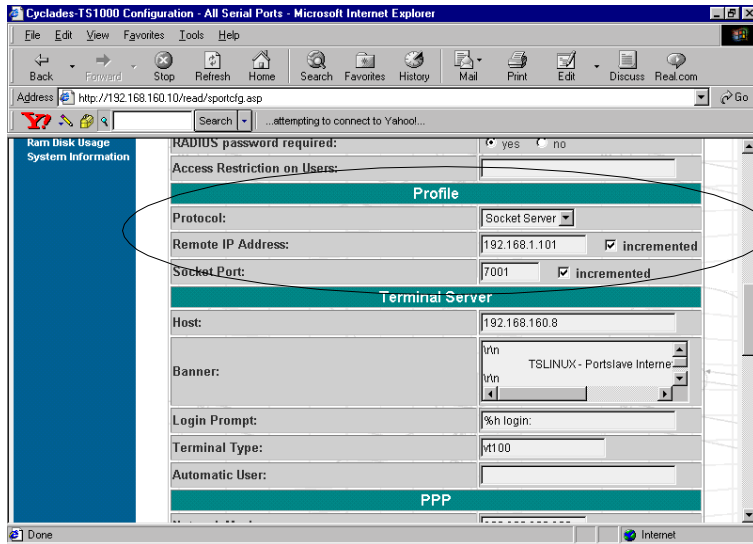


Figure 21: Profile Section of Serial Port Configuration page

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.

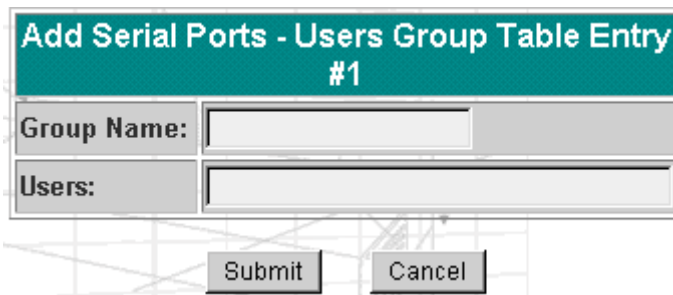
Chapter 3 - Additional Features

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.

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.



The image shows a web form titled "Add Serial Ports - Users Group Table Entry #1". The form has a teal header bar with the title in white text. Below the header, there are two input fields. The first is labeled "Group Name:" and the second is labeled "Users:". At the bottom of the form, there are two buttons: "Submit" and "Cancel". The form is overlaid on a faint grid background.

Figure 22: 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.

Go to the link Administration > Restart Processes and restart the cy_ras process.

Step 15: Save it in the flash.

Go to the link Administration > Load/Save Configuration and click the Save to Flash button.

Chapter 3 - Additional Features

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

Screen 2:

(Note: Screens 3 - 5 will all have the same instructions seen below, the instructions have been omitted intentionally.)

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

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

Chapter 3 - Additional Features

next parameter or

3) Press ESC if you want to exit.

ALL.IPNO - This is the default IP address of the system'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.

```
all.ipno[192.168.1.101+] :
```

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+] :
```

Chapter 3 - Additional Features

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, 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] :
```



Note: The modbus option only applies if you are using a TS100. Entering 'modbus' for your protocol displays the all.modbus_smode parameter.

ALL.MODBUS_SMODE - Communication mode through the serial ports. If not configured, ASCII mode will be assumed.(e.g. ascii -normal TX/RX mode, rtu -Remote Transmission mode where sometimes 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.

Chapter 3 - Additional Features

(e.g. !joe, mark, grp1 -the users, Joe, Mark, and members of grp1, cannot access the port.)

```
all.users[#] :
```

Screen 4:

```
*****  
***** 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[1000] :
```

ALL.TX_INTERVAL - Valid for protocols socket_server and raw_data. This parameter 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 0 or a value above 1000, no buffering will take place.

```
all.tx_interval[100] :
```

Screen 5:

```
*****  
***** 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

Chapter 3 - Additional Features

off. If set to 0 (the default), the connection will not time out.

```
all.idletimeout[0] :
```

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 6:

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

Your current configuration parameters are:
(The ones with the '#' means it's not activated.)

```
all.ipno : 192.168.1.101+  
all.socket_port : 7001+  
all.protocol : socket_server  
all.modbus_smode : #  
all.users : #  
all.poll_interval : 1000  
all.tx_interval : 100  
all.idletimeout : 0  
conf.group : #
```

Are these configuration(s) all correct (Y)es or (N)o [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':

Chapter 3 - Additional Features

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.

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. For “wiz -ac cas,” an additional parameter is asked: serverfarm. 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 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] :

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 *****
*****
```

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: Bring up the CLI.

At the command prompt, type the following to bring up the CLI:

```
config
```

This will show the CLI prompt:

```
config@hostname>>
```

Step 2: Type the following after the CLI prompt.

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

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

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

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

Chapter 3 - Additional Features

To configure the `poll_interval`:

```
configure line <serial port number> interval <number>
```

To configure the `socket_port`:

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



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

```
configure line <serial port number> tty <string> protocol  
<string> interval <number> socket <number>
```

Step 3: To exit the CLI.

Type *exit* or *quit* after the CLI prompt.

Step 4: To activate your new configurations and save them to flash, type:

```
signal_ras hup
```

Step 5: Save the configuration by typing:

```
saveconf
```

Chapter 3 - Additional Features

Configuration for TS

Parameters and Passed Values

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

<i>all.host</i>	The IP address of the host to which the terminals will connect.
<i>all.protocol</i>	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.
<i>all.socket_port</i>	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.
<i>all.userauto</i> (unique to TS)	Username used when connected to a UNIX server from the user's serial terminal.
<i>all.prompt</i>	This text defines the format of the <i>login prompt</i> . Expansion characters can be used here. Example: %h login:.
<i>all.term</i>	This parameter defines the <i>terminal type</i> assumed when performing rlogin or telnet to other hosts.
<i>all.issue</i>	This text determines the format of the <i>login banner</i> 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.

Example for all.issue:

```
\r\n\  
Welcome to terminal server %h port S%p \n\  
\r\n
```

Chapter 3 - Additional Features

CLI Method

To configure certain parameters for a specific serial port.

Step 1: Bring up the CLI.

At the command prompt, type the following to bring up the CLI:

```
config
```

This will show the CLI prompt:

```
config@hostname>>
```

Step 2: Type the following after the CLI prompt.

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

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

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

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

To configure the socket_port:

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



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

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

Step 3: To exit the CLI.

Type *exit* or *quit* after the CLI prompt.

Step 4: To activate your new configurations and save them to flash, type:

```
signal_ras hup
```

Step 5: Save the configuration by typing:

```
saveconf
```

Chapter 3 - Additional Features

vi Method

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

Browser Method

Step 1: Follow the steps 1 to 4 in the section titled Configuration for CAS, "[Browser Method](#)" on page 73.

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

<i>Profile section:</i>	Protocol (telnet, ssh, rlogin or socket client) Socket port (23 for telnet, 22 for ssh, 513 for rlogin)
-------------------------	--

<i>Terminal Server section:</i>	Host (the name or the IP address of the host) Automatic User
---------------------------------	---

Step 3: Click the Submit button.

At this point, the configuration file is written in the RAMdisk.

Step 4: Make changes effective.

Go to the link Administration > Restart Processes and restart the `cy_ras` process.

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:

```
wiz --ac ts
```

Screen 1 will appear.

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

Screen 2:

Screen 2: (Note: Screens 2 and 3 have the same instruction set preceding the parameters as seen in the previous section. The instructions have been omitted for brevity's sake.)

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

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.SOCKET_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] :
```

Chapter 3 - Additional Features

Screen 3:

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

ALL.USERAUTO - Username used when connected to a Unix server from the user's serial terminal.

```
all.userauto[#] :
```

Screen 4:

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

Your current configuration parameters are:
(The ones with the '#' means it's not activated.)

```
all.protocol : rlogin
all.socket_port : 23
all.userauto : #
```

Are these configuration(s) all correct (Y)es or (N)o [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 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 7.

Screen 6:

```
*****  
***** 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] :

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 *****
*****
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]

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.*

- | | |
|--------------------|---|
| <i>confpppd</i> | Location of the ppp daemon with Radius. Default value:
/usr/local/sbin/pppd. |
| <i>confacility</i> | This value (0-7) is the Local facility sent to the syslog. The file /etc/syslogng/syslog-ng.conf contains a mapping between the facility number and the action. |
| <i>allipno</i> | 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. |

Chapter 3 - Additional Features

all.initchat Modem initialization string. Example value:
TIMEOUT 10 "" \d\ \dATZ \OK\r\n-ATZ-OK\r\n "" \ "" ATMO OK\R\N ""\
TIMEOUT 3600 RING "" \
STATUS Incoming %p:I.HANDSHAKE "" ATA\
TIMEOUT 60 CONNECT@ "" \
STATUS Connected %p:I.HANDSHAKE

all.autoppp 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).

all.autoppp Example value:
(cont.) %j novj \
proxyarp modem asyncmap 000A0000 \
noipx noccp login auth require-pap refusechap\
mtu %t mru %t \
cb-script /etc/portslave/cb_script \
plugin /usr/lib/libpsr.so

all.pppopt PPP options when user has already been authenticated.
Example value:
%i:%j novj \
proxyarp modem asyncmap 000A0000 \
noipx noccp mtu %t mru %t netmask%m \
idle %I maxconnect %T \
plugin /usr/lib/libpsr.so

all.protocol For the Dial-in configuration, the available protocols are PPP, SLIP and CSLIP.

s32.tty Example value: ttyS32.

Chapter 3 - Additional Features



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 73](#).

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.autoppp* 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.

Go to the link Administration > Restart processes and restart the `cy_ras` process.

Step 8: Save it in the flash.

Chapter 3 - Additional Features

Go to the link [Administration > Load/Save Configuration](#) and click the **Save to Flash** button.

CLI Method

To configure certain parameters for a specific serial port:

Step 1: Bring up the CLI.

At the command prompt, type the following to bring up the CLI:

```
config
```

This will show the CLI prompt:

```
config@hostname>>
```

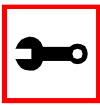
Step 2: Type the following after the CLI prompt:

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

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

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

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



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

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

Step 3: To exit the CLI.

Type *exit* or *quit* after the CLI prompt.

Step 4: To activate your new configurations and save them to flash, type:

```
signal_ras hup
```

Chapter 3 - Additional Features

Step 5: Save the configuration by typing:

```
saveconf
```

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* Type of authentication used. There are several authentication type options:
- *local* (authentication is performed using the `/etc/passwd` file)
 - *radius* (authentication is performed using a Radius authentication server)
 - *TacacsPlus* (authentication is performed using a TacacsPlus authentication server)
 - *none*
 - *local/radius* (authentication is performed locally first, switching to Radius if unsuccessful)
 - *radius/local* (the opposite of the previous option),
 - *RadiusDownLocal* (local authentication is tried only when the Radius server is down)
 - *local/TacacsPlus* (authentication is performed locally first, switching to TacacsPlus if unsuccessful)

Chapter 3 - Additional Features

- *TacacsPlus/local* (the opposite of the previous option), and
- *TacacsPlusDownLocal* (local authentication is tried only when the TacacsPlus server is down)
- *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`)

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`.

all.accthost1
all.accthost2

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.radtimeout

This is the timeout (in seconds) for a Radius/TacacsPlus 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.

Chapter 3 - Additional Features

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 73](#).

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.

Step 4: Make changes effective.

Go to the link Administration > Restart Processes and restart the `cy_ras` process.

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.

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

Screen 2:

(Note: Screens 2 through 5 have the same instruction set preceding the parameters as seen in the section for Access Method. The instructions have been omitted for brevity's sake.)

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

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] :
```



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.

Chapter 3 - Additional Features

ALL.AUTHHOST1 - This IP address indicates where the Radius or TacacsPlus authentication server is located.

```
all.authhost1[200.200.200.2] :
```

Screen 3:

```
*****  
***** 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] :
```

Screen 4:

```
*****  
***** 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] :
```

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.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[rad-secret] :
```

Screen 6:

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

Your current configuration parameters are:
(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)es or (N)o [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.

Chapter 3 - Additional Features

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.

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 *****
*****
You can now use the browser to finish your system configura-
tions, 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] :

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 *****  
*****
```

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: Bring up the CLI.

At the command prompt, type the following to bring up the CLI:

```
config
```

This will show the CLI prompt:

```
config@hostname>>
```

Step 2: Type the following after the CLI prompt.

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

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

To configure authtype:

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

Chapter 3 - Additional Features



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

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

Step 3: To exit the CLI.

Type *exit* or *quit* after the CLI prompt.

Step 4: To activate your new configurations and save them to flash, type:

```
signal_ras hup
```

Step 5: Save the configuration by typing:

```
saveconf
```

Chapter 3 - Additional Features

Clustering

Clustering is available for the Cyclades-TS with firmware versions 1.3.0 and up (except for the TS100). 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 512 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.

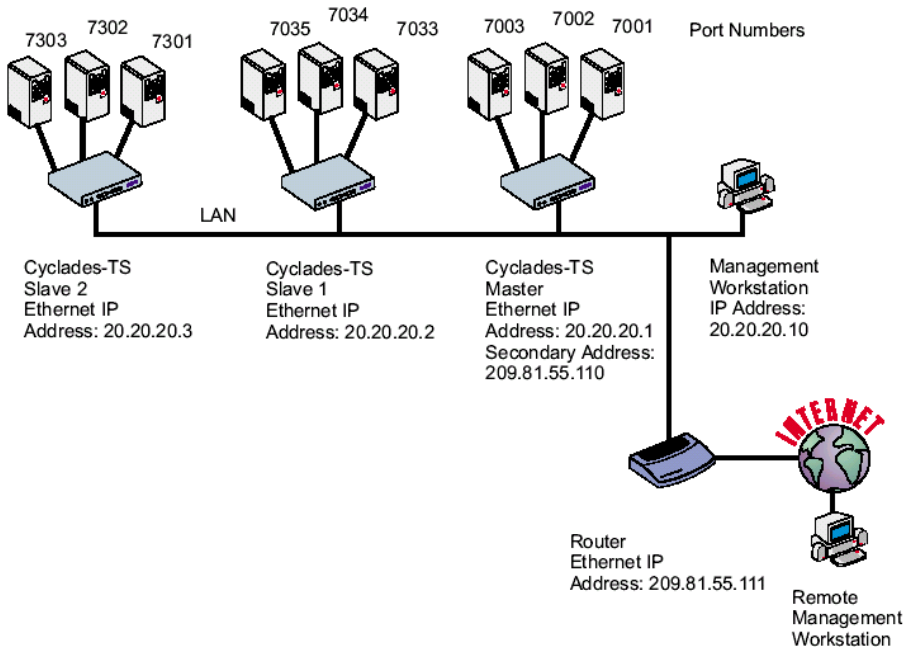


Figure 23: An example using the Clustering feature

Chapter 3 - Additional Features

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 6: Master Cyclades Configuration (where it differs from the CAS standard)

Parameter	Description	Value for this example
conf.eth_ip	Ethernet Interface IP address.	20.20.20.1
conf.eth_ip_alias	Secondary IP address for the Ethernet Interface (needed for clustering feature).	209.81.55.110
conf.eth_mask_alias	Mask for secondary IP address above.	255.255.255.0
all.socket_port	This value applies to both the local ports and ports on slave Cyclades-TS.	7001+
all.protocol	Depends on the application.	Socket_ssh or socket_server
all.authtype	Depends on the application.	Radius or local or none
s33.tty	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.	20.20.20.2:7033
s33.serverfarm	An alias for this port.	Server_on_slave1_serial_s1
s33.ipno	This parameter must be created in the master TS file for every slave port, unless configured using all.ipno.	0.0.0.0
s34.tty	See s33.tty.	20.20.20.2:7034

Chapter 3 - Additional Features

Table 6: Master Cyclades Configuration (where it differs from the CAS standard)

Parameter	Description	Value for this example
s34.serverfarm	An alias for this port.	Server_on_slave1_serial_s2
s34.ipno	See s33.ipno.	0.0.0.0
s35.tty	See s33.tty.	20.20.20.2:7035
s35.serverfarm	An alias for this port.	Server_on_slave1_serial_s3
s35.ipno	See s33.ipno.	0.0.0.0
etc. for s36-s64		
S65.tty	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.	20.20.20.3:7301
S65.serverfarm	An alias for this port.	Server_on_slave2_serial_s1
S65.ipno	See s33.ipno.	0.0.0.0
S66.tty	See s65.tty	20.20.20.3:7302
S66.serverfarm	An alias for this port.	Server_on_slave2_serial_s2
S66.ipno	See s33.ipno.	0.0.0.0
S67.tty	See s65.tty.	20.20.20.3:7303
S67.serverfarm	An alias for this port.	Server_on_slave2_serial_s3
S67.ipno	See s33.ipno.	0.0.0.0
etc. for s68-s96		

Chapter 3 - Additional Features

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

Parameter	Value for this example
all.protocol	socket_server
all.authtype	none
conf.eth_ip	20.20.20.2
all.socket_port	7033+
all.authtype	none

Table 8: Cyclades-TS configuration for Slave 2
(where it differs from the CAS standard)

Parameter	Value for this example
all.protocol	socket_server
all.authtype	none
conf.eth_ip	20.20.20.3
all.authtype	none
all.socket_port	7301+

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.

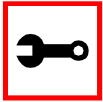
Chapter 3 - Additional Features

```
telnet 209.81.55.110 7033
```

to access the first port of Slave 1.

```
telnet 209.81.55.110 7065
```

to access the first port of Slave 2.



Note. Socket port 7065 is being used in the last example to access port 7301 in 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>:7069 209.81.55.110
```

to access the fifth port of Slave 2.

Centralized Management - the Include File

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 [Figure 24: Example of Centralized Management](#), is `/etc/portslave/TSccommon.conf`. It must be downloaded to each Cyclades-TS.

Chapter 3 - Additional Features

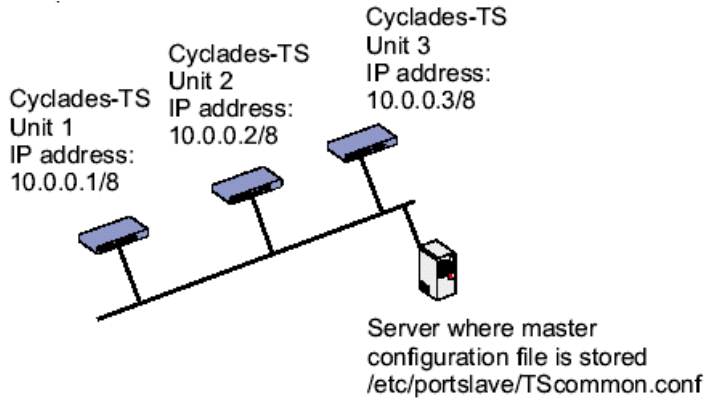


Figure 24: Example of Centralized Management

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

For the `/etc/hostname` file in *unit 1*:

```
unit1
```

For the `pslave.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 `pslave.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
```

Chapter 3 - Additional Features

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

```
unit3
```

For the `pslave.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:

```
conf.host_config unit1
<parameters for unit1 following the rules for pslave.conf>
conf.host_config unit2
<parameters for unit2 following the rules for pslave.conf>
conf.host_config unit3
<parameters for unit3 following the rules for pslave.conf>
conf.host_config.end
```

When this file is included, *unit1* would read only the information between *conf.host_config unit1* and *conf.host_config unit2*. *Unit2* would use only the information between *conf.host_config unit2* and *conf.host_config unit3* and *unit3* would use information after *conf.host_config unit3* and before *conf.host_config.end*.

Steps for using Centralized Configuration

Step 1: Create and save the `/etc/portslave/pslave.conf` and `/etc/hostname` files in each Cyclades-TS.

Step 2: Execute the command `signal_ras hup` on each unit.

Chapter 3 - Additional Features

Step 3: Create, save, and download the common configuration.

Create and save the common configuration file on the server, then download it (probably using `scp`) to each unit. Make sure to put it in the directory set in the `pslave.conf` file (`/etc/portslave` in the example).

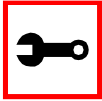
Step 4: Execute the command `signal_ras hup` on each unit again.

Step 5: Test each unit.

If everything works, add the line `/etc/portslave/TScommon.conf` to the `/etc/config_files` file.

Step 6: Save the file and close it.

Step 7: Execute the `saveconf` command.



Note: The included file `/etc/portslave/TScommon.conf` cannot contain another include file (i.e., the parameter `conf.include` must not be defined).

Also, `<max ports of TS> + N(+)` is done same way as serial port.

Chapter 3 - Additional Features

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/test_cron.sh
```

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

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

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

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 TS.

In the address field of your browser, type:

<Console Access Server's IP address>

Chapter 3 - Additional Features

Step 2: Log in.

Log in as root, pwd is tslinux. 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.

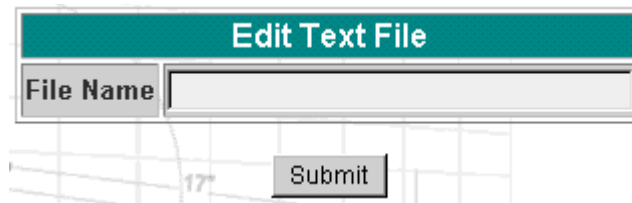


Figure 25: Edit Text File page

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_dat_buffering is a remote network file system where data buffering will be written, instead of using the default directory */var/run*. When commented, it indicates local data buffering. The directory tree to which the file will be written must be NFS-mounted and the local pathname 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 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 *<serverfarm1>.data* if *s1.serverfarm* was configured) in local directory */va/run* or in remote pathname 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 4 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*.

Chapter 3 - Additional Features

Parameters Involved and Passed Values

Data Buffering uses the following parameters:

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.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.

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.

Chapter 3 - Additional Features

Configuration for CAS

vi Method

Files to be modified:

- pslave.conf
- syslog-ng.conf

Browser Method

To configure Data Buffering with your browser:

Step 1: Point your browser to the TS.

In the address field of your browser type:

`<Console Access Server's IP address>`

Step 2: Log in.

Log in as root, pwd is tslinux. 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.

Chapter 3 - Additional Features

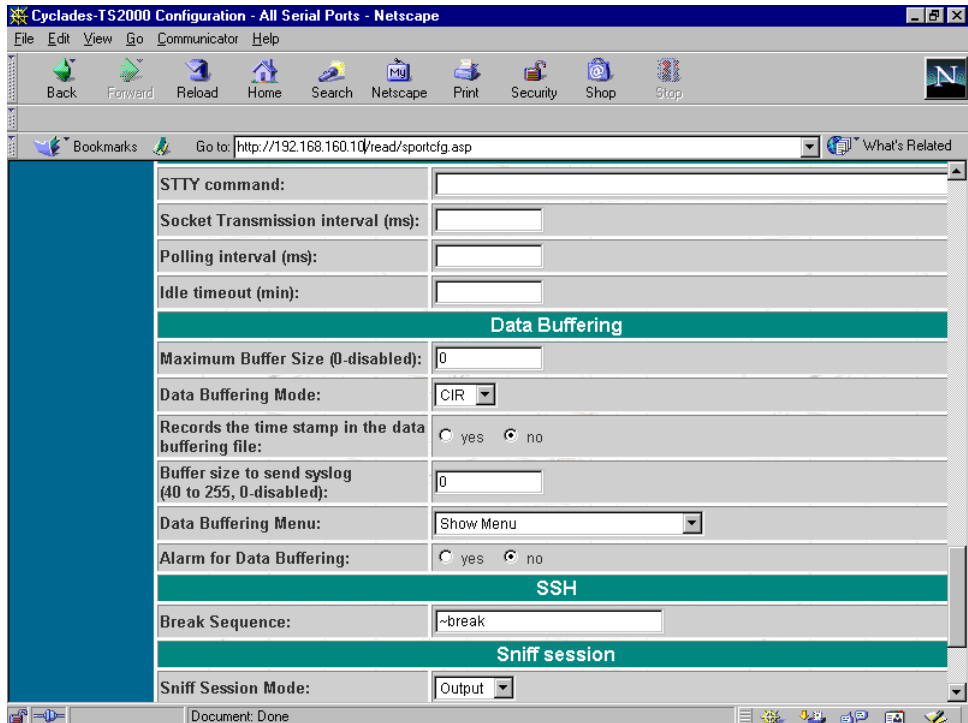


Figure 26: Data Buffering section of the Serial Port Configuration page

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.

Chapter 3 - Additional Features

Data Buffering	
Remote NFS path:	<input type="text"/>
Data Buffering Facility:	local7 <input type="button" value="v"/>

Figure 27: Data Buffering section of the General page

Step 9: Click the Submit button.

Step 10: Click on Administration > Restart Processes > signal_ras hup.
The new configuration is now running.

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:

```
*****  
***** C O N F I G U R A T I O N   W I Z A R D *****  
*****  
Set to defaults ? (y/n) [N] :
```

Chapter 3 - Additional Features

Screen 2:

(Note: Screens 2 through 4 have the same instruction set preceding the parameters as seen in the section for Access Method. The instructions have been omitted for brevity's sake.)

```
*****  
***** 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 3:

```
*****  
***** 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

Chapter 3 - Additional Features

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 4:

```
*****  
***** 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, an 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

Chapter 3 - Additional Features

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 5:

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

Your current configuration parameters are:
(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
```

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



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 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 :

Screen 7:

```
*****
***** 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] :

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

Chapter 3 - Additional Features

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]

DHCP

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/dhcpd_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):

Chapter 3 - Additional Features

- 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/dhcpd_cmd
```

(from factory file already present in `/etc/config_files`)

```
/etc/dhcpd-eth0.save
```

(from factory file already present in `/etc/config_files`)

- Add the option “-x” to the factory default content of the file `/etc/network/dhcpd_cmd`:

```
/bin/dhcpd -x -c /bin/handle_dhcp
```

From the factory, `/etc/network/dhcpd_cmd` has already has such content.

- Add all other necessary options to the file `/etc/network/dhcpd_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/dhcpd_cmd`

Contains a command that activates the DHCP client (used by the `cy_ras` program). Its factory contents are:

```
/bin/dhcpd -c /bin/handle_dhcp
```

Chapter 3 - Additional Features

The options available that can be used on this command line are:

- D** This option forces dhcpd 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 dhcpd 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 dhcpd from replacing the existing `/etc/resolv.conf` file.



Note. Do not modify the `-c /bin/handle_dhcp` option.

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 theTS.

In the address field of your browser type:

`<Console Access Server's IP address>`

Step 2: Log in.

Log in as `root`, `pwd` is `tslinux`. This will take you to the Configuration and Administration page.

Chapter 3 - Additional Features

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.

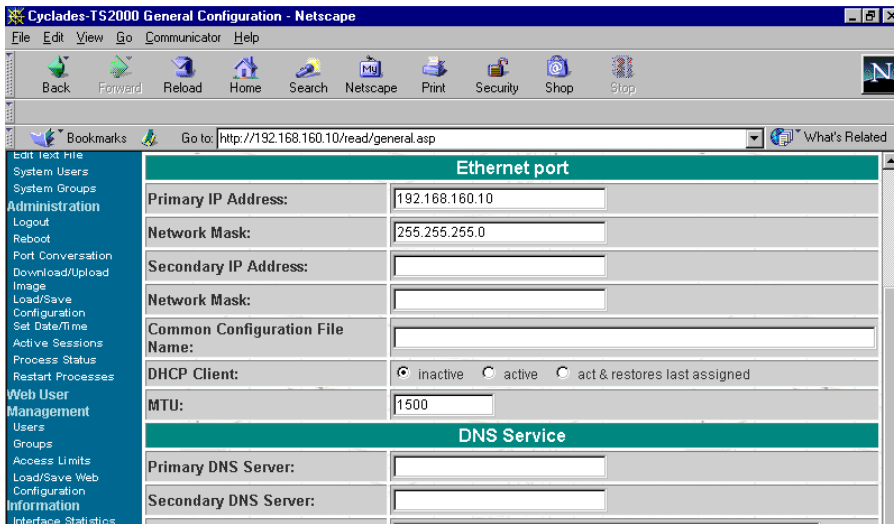


Figure 28: DHCP client section

Step 5: Click on Administration > Restart Processes > signal_ras hup.

If you enabled or 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 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) or the how-to:

<http://www.netfilter.filewatcher.org/ipchains/HOWTO.html>

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:

<i>input</i>	Filters for packets coming into the Cyclades-TS itself.
<i>output</i>	Filters for locally-generated packets.
<i>forward</i>	Filters for packets being routed through the Cyclades-TS.
<i>user_created_chain</i>	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.

Chapter 3 - Additional Features

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 field of your browser type:

<Console Access Server's IP address>

Step 2: Log in.

Log in as *root*, with *tslinux* as a password. This will take you to the Configuration and Administration page. (See [“Configuration & Administration Menu page” on page 40](#))

Step 3: Click IPChains filter link.

Click on this link on the Link Panel. The following page will appear:

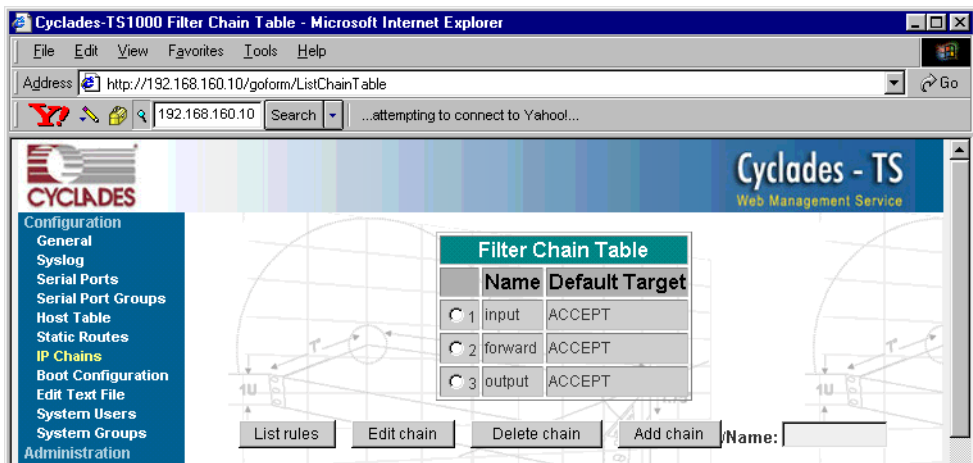


Figure 29: Page 1 of IP Chain filtering

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.

Chapter 3 - Additional Features

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

<i>conf:DB_facility</i>	This value (0-7) is the Local facility sent to the <code>syslog-ng</code> with data when <code>syslog_buffering</code> and/or <code>alarm</code> is active.
<i>all.alarm</i>	When nonzero, all data received from the port is captured and sent to <code>syslog-ng</code> with INFO level and <code>LOCAL[0+conf.DB_facility]</code> facility.

Chapter 3 - Additional Features

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 TS.

In the address field of your browser type:

```
<Console Access Server's IP address>
```

Step 2: Log in.

Log in as root, pwd is tslinux. This will take you to the Configuration and Administration page.

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.

Chapter 3 - Additional Features

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: Click on Administration > Restart Processes > signal_ras hup.

The new configuration is running.

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.

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 *****  
*****
```

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

Chapter 3 - Additional Features

Screen 2:

(Note: Screens 2 has the same instruction set preceding the parameters as seen in the section for Access Method. The instructions have been omitted for brevity's sake.)

```
*****  
***** 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).

Screen 3:

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

Your current configuration parameters are:
(The ones with the '#' means it's not activated.)

```
all.alarm : 0
```

```
Are these configuration(s) all correct (Y)es or (N)o [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':

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

Typing 'c' leads to Screen 4, typing 'q' leads to Screen 5.

Screen 4:

```
*****
***** 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 5.

Screen 5:

```
*****
***** 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

Chapter 3 - Additional Features

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 6:

```
*****  
***** 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]

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 src { unix-stream("/dev/log"); };  
  
# To filter ALARM message with the string "kernel panic" :
```

Chapter 3 - Additional Features

```
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
# of this unit and the message that was received from the
source.

destination d_maill {
    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 thisTS 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 :
```

Chapter 3 - Additional Features

```
destination d_trap {
pipe("/dev/cyc_alarm"
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\" "););
};

# To send e-mail and snmptrap if message received from local
syslog client has the string "kernel panic" :

log { source(sysl); filter(f_kpanic); destination(d_maill);
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_maill);
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):

Chapter 3 - Additional Features

```
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.

```
log (source(sysl); filter(f_kpanic); destination(d_pager);
};
```

To send e-mail:

```
destination d_mail { pipe("/dev/cyc_alarm" template("send-
mail <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); );
```

Chapter 3 - Additional Features

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.

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:

<i>-t <name>[,<name>]</i>	“To: ” Required. Multi-part allowed (multiple names are separated by commas). Names are expanded as explained below.
<i>[-c <name> [,<name>]]</i>	“Cc: ” Optional. Multi-part allowed (multiple names are separated by commas).
<i>[-b <name> [,<name>]]</i>	“Bcc: ” Optional. Multi-part allowed (multiple names are separated by commas).
<i>[-r <name>]</i>	“Reply-To: ” Optional. Use the Reply-To: field to make sure the destination user can send a reply to a regular mailbox.
<i>-f <name></i>	“From: ” Required.
<i>-s <text></i>	“Subject: ” Required.
<i>-m <text></i>	“body” The message body.
<i>-h <SMTP server></i>	Required. IP address or name of the SMTP server.
<i>[-p <SMTP port></i>	Optional. The port number used in the connection with the server. Default: 25.
<i><name></i>	Any email address.
<i><text></i>	A text field. As this kind of field can contain blank spaces, please use the quotation marks to enclose the text.

Chapter 3 - Additional Features

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
```

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.

Chapter 3 - Additional Features

- 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. In case of doubt, 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).

Chapter 3 - Additional Features

-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.

server Required. The host name or IP address of the computer where the SMS gateway server process is running. By default, this server will be listening on TCP port 6701.

Upon success (when the server module reports that the message was successfully sent), sendsms returns 0. When a problem occurs, a non zero value is returned. Different return values indicate different problems. A return value of 1 indicates a general failure of the client program.

COPYRIGHT: SMSLink is (c) Les Ateliers du Heron, 1998 by Philippe Andersson.

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
```

Snmpttrap

Snmpttrap 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]...
```

Chapter 3 - Additional Features

where:

<i>-Ci</i>	Optional. It sends INFORM-PDU.
<i>common arguments</i>	Required. They are: "-c <community name> <SNMP server IP address>"
<i>enterprise-oid</i>	Required, but it can be empty (").
<i>agent</i>	Required, but it can be empty ("). The agent name.
<i>generic-trap</i>	The generic trap number: 2 (link down), 3 (link up), 4 (authentication failure), ...
<i>specific-trap</i>	Required. The specific trap number.
<i>uptime</i>	Required.
<i>[objectID type value]</i>	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:

```
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"
```

<i>-Ci</i>	Optional. It sends INFORM-PDU.
<i>common arguments</i>	Required. They are: SNMP server IP address and community.
<i>enterprise-oid</i>	Required, but it can be empty (").

Chapter 3 - Additional Features

Help

Help Wizard Information

Synopsis: `wiz [--OPTIONS] [--port <port number>]`



Note: Make sure there are two hyphens before any of the options listed on the following table.

Table 9: General Options for the Help Wizard

Option	Description
<i>auth</i>	Configuration of authentication parameters
<i>tl</i>	Configuration of terminal login display parameters
<i>al</i>	Configuration of alarm parameter
<i>db</i>	Configuration of data buffering parameters
<i>snf</i>	Configuration of sniffing parameters
<i>sl</i>	Configuration of syslog parameters
<i>tso</i>	Configuration of other parameters specific to the TS profile
<i>ac</i> <cas or ts>	Configuration of access method parameters
<i>sset</i> <cas or ts>	Configuration of serial setting parameters
<i>all</i> <cas or ts>	Configuration of all parameters
<i>help</i>	Print this help message

Step 1: Bring up the wizard.

Chapter 3 - Additional Features



Note: To directly configure a feature for a specific serial port, use the “-port <port number>” option after “wiz -[option].”

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

Synopsis 1

```
config configure line [serial port number] [options]
```

or

```
configure line [serial port number] [options]
```

(The command above is valid only after entering into CLI mode. This is done by first just typing `config` at the terminal prompt. Then you will get a CLI prompt such as `config@host-name>>`. Once in the CLI mode, you eliminate the need to type `config` in all your CLI commands.)

Table 10: Help CLI Options - Synopsis 1

Option	Description
<i>tty</i> <string>	Activate the serial port.
<i>protocol</i> <string>	Configuration of protocol for the serial port.
<i>interval</i> <number>	Configuration of poll_interval for the serial port.
<i>authtype</i> <string>	Configuration of authentication type for the serial port.
<i>speed</i> <number>	Configuration of speed for the serial port.

Chapter 3 - Additional Features

Table 10: Help CLI Options - Synopsis 1

Option	Description
<i>datasize</i> <number>	Configuration of datasize for the serial port.
<i>stopbits</i> <number>	Configuration of the stopbits for the serial port.
<i>parity</i> <string>	Configuration of the parity for the serial port.
<i>socket</i> <number>	Configuration of socket_port for the serial port.
<i>break</i> <string>	Configuration of break_sequence for the serial port.

There are also other options that configures network related parameters.

Synopsis 2

```
config configure ether [options]
```

or

```
configure ether [options]
```

(This synopsis is valid only after entering into CLI mode. This is done by first just typing `config` at the terminal prompt. Then, you will get a CLI prompt such as `config@hostname>>`.)

Table 11: Help CLI Options - Synopsis 2

Option	Description
<i>ip</i> <string>	Configuration of the IP of the Ethernet interface.
<i>mask</i> <string>	Configuration of the mask for the Ethernet network
<i>mtu</i> <number>	Configuration of the Maximum Transmission Unit size

Chapter 3 - Additional Features

Requesting Help for the CLI

There are two methods for requesting help for the CLI:

- To obtain general help on the format of CLI, type *config help* at the command prompt, or if you are already in the CLI, just type *help* after the CLI 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> ?
```

Modbus

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 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).

Chapter 3 - Additional Features

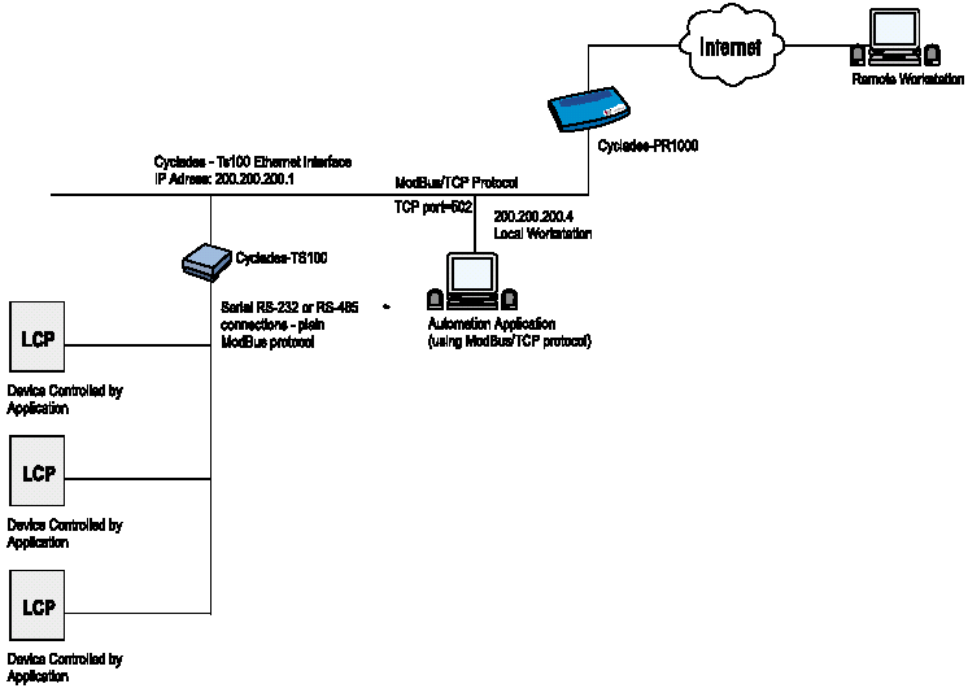


Figure 30: Modbus application

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-TS100 using MODBUS/TCP protocol. The connection is opened using Cyclades-TS100 Ethernet IP address and TCP port = 502. Cyclades-TS100 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:

Chapter 3 - Additional Features

Table 12: Modbus pslave.conf port-specific parameters
(only where they differ from the standard CAS profile)

Parameter	Description	Value for this Example
all.authtype	<p>Type of authentication used. There are several authentication type options:</p> <ul style="list-style-type: none">• <i>local</i> (authentication is performed using the /etc/passwd file)• <i>radius</i> (authentication is performed using a Radius authentication server)• <i>TacacsPlus</i> (authentication is performed using a TacacsPlus authentication server)• <i>none</i>• <i>local/radius</i> (authentication is performed locally first, switching to Radius if unsuccessful)• <i>radius/local</i> (the opposite of the previous option),• <i>RadiusDownLocal</i> (local authentication is tried only when the Radius server is down)• <i>local/TacacsPlus</i> (authentication is performed locally first, switching to TacacsPlus if unsuccessful)	none

Chapter 3 - Additional Features

Table 12: Modbus pslave.conf port-specific parameters
(only where they differ from the standard CAS profile)

Parameter	Description	Value for this Example
all.authtype (cont.)	<ul style="list-style-type: none">• <i>TacacsPlus/local</i> (the opposite of the previous option), and• <i>TacacsPlusDownLocal</i> (local authentication is tried only when the TacacsPlus server is down)• <i>ldap</i> (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 <code>/etc/ldap.conf</code>) <p>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.</p>	
all.socket_port	This defines an alternative labeling system for the Cyclades-TS ports. The '+' after the numerical value causes the interfaces to be numbered consecutively. In this example, interface 1 is assigned the port value 7001, interface 2 is assigned the port value 7002, etc.	502
all.protocol	For the console server profile, the possible protocols are <code>socket_server</code> (when telnet is used), <code>socket_ssh</code> (when ssh version one or two is used), <code>raw_data</code> (to exchange data in transparent mode – similar to <code>socket_server</code> mode, but without telnet negotiation, breaks to serial ports, etc.), or <i>modbus</i> (an application layer messaging protocol for client/server communication widely used for industrial automation).	modbus

Chapter 3 - Additional Features

Table 12: Modbus pslave.conf port-specific parameters
(only where they differ from the standard CAS profile)

Parameter	Description	Value for this Example
all.smode	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.	ascii

NTP

The `ntpcient` is a *Network Timer 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/ntpcient.conf`.

The script shell `/bin/ntpcient.sh` reads the configuration file (`/etc/ntpcient.conf`) and build the line command to call `/bin/ntpcient` program.

Parameters Involved and Passed Values

The file `/etc/ntpcient.conf` has the value of two parameters:

NTPSERVER The IP address of the NTP server.
INTERVAL Check time every interval seconds (default 300).

The data and time will be update from the NPT server according to the parameter options.

The `ntpcient` program has this syntax:

```
ntpcient [options]
```

Chapter 3 - Additional Features

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.
- r* Replay analysis code based on stdin.
- s* Clock set (if count is not defined this sets count to 1).

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 TS.

In the address field of your browser type:

```
<Console Access Server's IP address>
```

Step 2: Log in.

Log in as root, pwd is tslinux. 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 11: Configuration & Administration Menu page](#). You can then pull up the appropriate file and edit it.

Chapter 3 - Additional Features

Ports Configured for 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.

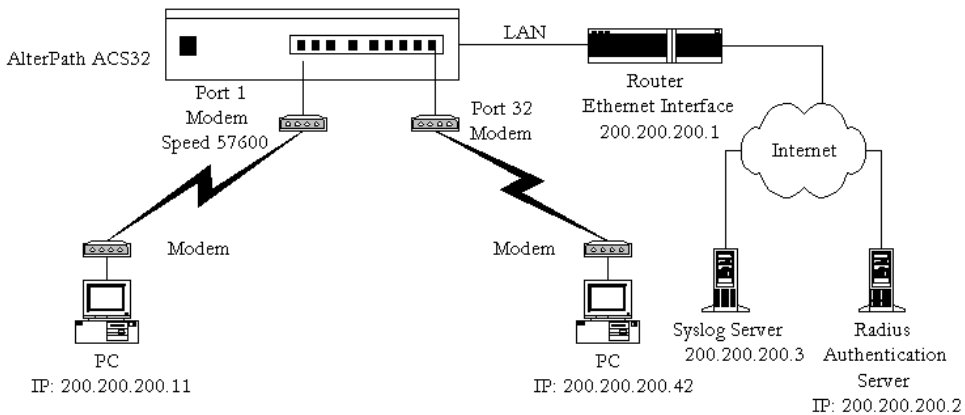


Figure 31: Ports configured for Dial-in Access

In addition to the parameters which are common to all setups, and which appear in [Appendix C - The pslave Configuration File](#), you may also configure additional parameters if you wish to configure some ports for Dial-in Access. These are also listed in the same section under [Dial-in Access Parameters](#). After configuring the desired parameters, execute the command `signal_ras hup` to activate the changes. At this point, the configuration should be tested. A step-by-step check list follows:

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*.

Chapter 3 - Additional Features

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 and Configuration](#).



Important! TS100 owners: please skip to the special section on the TS100 later in the installation chapter Configuring the Cyclades-TS100 for the first time, then perform [“Task 5: Activate the changes” on page 59](#) through [“Task 8: Reboot the Cyclades-TS” on page 60](#) listed in Chapter 2 - Installation and Configuration to finish the configuration. Make into links.

Chapter 3 - Additional Features

Ports Configured as Terminal Servers

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.

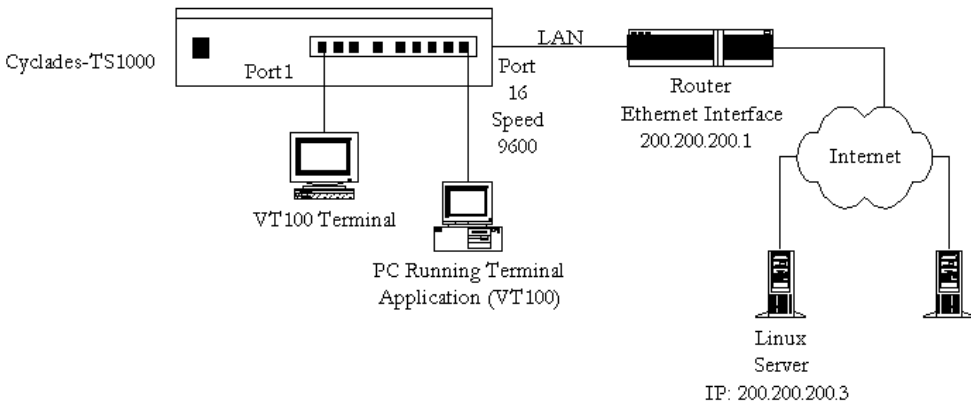


Figure 32: Terminal Server diagram

In addition to the parameters which are common to all setups, and which are listed in [Appendix C - The pslave Configuration File](#), you may also configure additional parameters for the Terminal Server port profile. They are listed in the same chapter under [TS Parameters](#).

Chapter 3 - Additional Features

TS Setup Scenario

No authentication is used in the example shown in [Figure 32: Terminal Server diagram](#) and rlogin is chosen as the protocol. After configuring the desired parameters, execute the command *signal_ras_hup* to activate the configuration changes. At this point, the configuration should be tested. A step-by-step check list follows:

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 [Task 8: Reboot the Cyclades-TS](#) listed in [Chapter 2 - Installation and Configuration](#).

Chapter 3 - Additional Features

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:

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

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

Screen 2:

(Note: Screens 2 and 3 have the same instruction set preceding the parameters as seen in the section for Access Method. The instructions have been omitted for brevity's sake.)

```
*****
***** 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[200.200.200.3] :

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 3:

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

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 4:

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

Your current configuration parameters are:
(The ones with the '#' means it's not activated.)

```
all.host : 200.200.200.3
all.term : vt100
conf.locallogins : 0
```

Are these configuration(s) all correct (Y)es or (N)o [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':

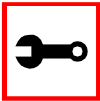
Type 'c' to CONTINUE to set these parameters for
specific ports or 'q' to QUIT :

Chapter 3 - Additional Features

Typing 'c' leads to Screen 5, typing 'q' leads to Screen 6.

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 :
```



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 6.

Screen 6:

```
*****
***** 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] :

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 *****  
*****
```

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]

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):

<i>all.speed</i>	The speed for all ports. Default value: <i>9600</i> .
<i>all.datasize</i>	The data size for all ports. Default value: <i>8</i> .
<i>all.stopbits</i>	The number of stop bits for all ports. Default value: <i>1</i> .
<i>all.parity</i>	The parity for all ports. Default value: <i>none</i> .
<i>all.flow</i>	This sets the flow control to hardware, software, or none. Default value: <i>none</i> .

Chapter 3 - Additional Features

all.dcd (for CAS only)

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.

all.sttyCmd

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 value specifies how long (in milliseconds) a DTR signal will be turned off before it is turned back on again. If set to 0, this parameter will NOT be active. This may be dangerous if a user were to connect to a port that a previous user was on but had lost the session after a timeout. The user may directly connect into the previous user's shell. A minimum of 100ms is required otherwise it is assumed.

Chapter 3 - Additional Features

Configuration for CAS

Browser Method

Step 1: Point your browser to the TS.

In the address field of your browser type:

<Console Access Server's IP address>

Step 2: Log in.

Log in as root, pwd is tslinux. 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 Physical section.

You can change the settings for Speed, Data Size, Stop Bit, Parity, Flow Control, and DCD-sensitivity here.

Step 6: Click on the Submit button.

Step 7: Click on Administration > Restart Processes > signal_ras hup.

The new configuration is now running.

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.

Chapter 3 - Additional Features

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.

Screen 1:

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

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

Screen 2:

(Note: Screens 2 through 5 have the same instruction set preceding the parameters as seen in the section for Access Method. The instructions have been omitted for brevity's sake.)

```
*****  
***** 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] :
```

Chapter 3 - Additional Features

Screen 3:

```
*****  
***** 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 4:

```
*****  
***** 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] :
```

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.DTR_RESET - This parameter specifies how long (in milliseconds) a DTR signal will be turned off before it is turned on again. If set to 0, this parameter will NOT be active. This may be dangerous when a user connects to a port that a previous user was on but had lost the session after a timeout. The user may directly connect into the previous user's shell. A minimum of 100ms is required.

```
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 6:

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

Your current configuration parameters are:
(The ones with the '#' means it's not activated.)

```
all.speed : 9600
all.datasize : 8
all.stopbits : 1
all.parity : none
all.flow : none
```

Chapter 3 - Additional Features

```
all.dcd : 0
all.DTR_reset : 100
all.sttyCmd : #
```

Are these configuration(s) all correct (Y)es or (N)o [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.

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.

Chapter 3 - Additional Features

Screen 8:

```
*****
***** 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] :

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]

Chapter 3 - Additional Features

CLI Method

To configure certain parameters for a specific serial port.

Step 1: Bring up the CLI.

At the command prompt, type the following to bring up the CLI:

```
config
```

This will show the CLI prompt:

```
config@hostname>>
```

Step 2: Type the following after the CLI prompt:

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

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

To configure speed:

```
configure line <serial port number> speed <number>
```

To configure datasize:

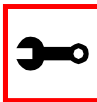
```
configure line <serial port number> datasize <number>
```

To configure stopbits:

```
configure line <serial port number> stopbits <number>
```

To configure parity:

```
configure line <serial port number> parity <string>
```



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

```
configure line <serial port number> tty <string> speed  
<number> datasize <number> stopbits <number> parity  
<string>
```

Chapter 3 - Additional Features

Step 3: To exit the CLI.

Type *exit* or *quit* after the CLI prompt.

Step 4: To activate your new configurations and save them to flash, type:

```
signal_ras hup
```

Step 5: Save the configuration by typing:

```
saveconf
```

Configuration for TS

Browser Method

See the browser method for the CAS, earlier in this section.

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
```



Note: Screens 1- 4 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. In the TS configuration, sttyCmd is not requested.

Screen 5:

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

Your current configuration parameters are:
(The ones with the '#' means it's not activated.)

Chapter 3 - Additional Features

```
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)es or (N)o [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 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 *****
*****
```

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] :

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]

Chapter 3 - Additional Features

CLI Method

To configure certain parameters for a specific serial port.

Step 1: Bring up the CLI.

At the command prompt, type the following to bring up the CLI:

```
config
```

This will show the CLI prompt:

```
config@hostname>>
```

Step 2: Type the following after the CLI prompt:

This activates the serial port. <string> should be “ttyS<serial port number>”:

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

To configure speed:

```
configure line <serial port number> speed <number>
```

To configure datasize:

```
configure line <serial port number> datasize <number>
```

To configure stopbits:

```
configure line <serial port number> stopbits <number>
```

To configure parity:

```
configure line <serial port number> parity <string>
```



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

```
configure line <serial port number> tty <string> speed  
<number> datasize <number> stopbits <number> parity  
<string>
```

Chapter 3 - Additional Features

Step 3: To exit the CLI.

Type *exit* or *quit* after the CLI prompt.

Step 4: To activate your new configurations and save them to flash, type:

```
signal_ras hup
```

Step 5: Save the configuration by typing:

```
saveconf
```

Configuration for Dial-in Access

The parameters are the same as before.

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>) !!!
```

Chapter 3 - Additional Features

*

- 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).

Versions 1.3.3 and later

Users will be able to 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 simultaneous users can sniff the session or have read and/or write permission. Default value: no.
- **sN.multiple_sessions**: Valid only for port N; must be “yes” or “no.” If it is not defined, it will assume the value of **all.multiple_sessions**.
- **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**.

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):

Chapter 3 - Additional Features

```
*
* * * 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 "all" to kill all the sessions. If the administrator kills all the regular sessions, his session initiates as a regular session automatically.

Chapter 3 - Additional Features

Option 5 - Quit will close the current session and the TCP connection.

Only for the administrator users:

Typing *all.escape_char* or *sNescape_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:

- | | |
|------------------------------|---|
| <i>all.admin_users</i> | 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 <i>authtype</i> must not be none. User groups (defined with the parameter <i>conf.group</i>) can be used in combination with user names in the parameter list. Example values: peter, john, user_group. |
| <i>all.sniff_mode</i> | This parameter determines what other users connected to the very same port (see parameter <i>admin_users</i> below) can see of the session of the first connected user (main session): <i>in</i> shows data written to the port, <i>out</i> shows data received from the port, and <i>i/o</i> shows both streams. The second and later sessions are called sniff sessions and this feature is activated whenever the protocol parameter is set to <i>socket_ssh</i> or <i>socket_server</i> . Example value: out. |
| <i>all.escape_char</i> | This parameter determines which character must be typed to make the session enter <i>menu mode</i> . The possible values are <CTRL-a> to <CTRL-z>. Represent the CTRL with caret: ^. This parameter is only valid when the port protocol is <i>socket_server</i> or <i>socket_ssh</i> . Default value is ^z. |
| <i>all.multiple_sessions</i> | Must be <i>yes</i> or <i>no</i> . If it is configured as no, 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 and/or write permission. Default value: no. |

Chapter 3 - Additional Features

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 TS.

In the address field of your browser type:

`<Console Access Server's IP address>`

Step 2: Log in.

Log in as *root*, *pwd* is *tslinux*. 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.

Sniff session	
Sniff Session Mode:	Output ▾
Administrative Users:	<input type="text"/>
Escape char from sniff mode:	<input type="text"/>
Allows multiple sniff sessions:	<input type="radio"/> yes <input checked="" type="radio"/> no

Chapter 3 - Additional Features

Figure 33: Sniff Session section of the Serial Port Configuration page

Step 6: Click on the Submit button.

Step 7: Click on Administration > Restart Processes > signal_ras hup.
The new configuration is now running.

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
```

Screen 1:

```
*****
***** C O N F I G U R A T I O N   W I Z A R D *****
*****
Set to defaults ? (y/n) [N] :
```

Screen 2:

(Note: Screens 2 and 3 have the same instruction set preceding the parameters as seen in the section for Access Method. The instructions have been omitted for brevity's sake.)

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

Chapter 3 - Additional Features

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] :

Screen 3:

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

ALL.ESCAPE_CHAR - This parameter determines which character must be typed to make the session enter into "menu mode." The possible values are <CTRL-a> to <CTRL-z>, and this is only valid when the port protocol is socket_server or socket_ssh. Represent the CTRL

Chapter 3 - Additional Features

character with '^'. Default value is ^z.

all.escape_char[^z] :

ALL.MULTIPLE_SESSIONS - Allow users to open more than one common and sniff sessions on the same port. The parameter must be a 'yes' or a 'no' to open. Default is set to 'no'.

all.multiple_sessions[no] :

Screen 4:

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

Your current configuration parameters are:
(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)es or (N)o [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 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 *****
*****
You can now use the browser to finish your system configura-
tions, 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] :

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 *****  
*****
```

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]

SNMP

Short for Simple Network Management Protocol: a set of protocols for managing complex networks. The first versions of SNMP were developed in the early 80s. SNMP works by sending messages, called protocol data units (PDUs), to different parts of a network. SNMP-compliant devices, called agents, store data about themselves in Management Information Bases (MIBs) and return this data to the SNMP requesters.

The TS uses the net-snmp package (<http://www.net-snmp.org>).

The net-snmp supports snmp version 1, 2 and 3. 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

Chapter 3 - Additional Features

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.)

Chapter 3 - Additional Features

Configuration for CAS, TS, and Dial-in Access

vi Method

Files to be changed:

```
/etc/snmp/snmpd.conf
```

This file has information about configuring for SNMP.

Browser Method

To configure SNMP with your browser:

Step 1: Point your browser to the TS.

In the address field of your browser type:

```
<Console Access Server's IP address>
```

Step 2: Log in.

Log in as *root*, pwd is *tslinux*. 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 11: Configuration & Administration Menu page](#). You can then pull up the appropriate file and edit it.

Syslog

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 the contents of them 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.

Chapter 3 - Additional Features

The configuration file (default: `syslog-ng.conf`) is read at startup and is reread after receipt 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 191](#).

Port Slave Parameters Involved with `syslog-ng`

<i>conf.facility</i>	This value (0-7) is the Local facility sent to the <code>syslog-ng</code> from <code>PortSlave</code> .
<i>conf.DB_facility</i>	This value (0-7) is the Local facility sent to the <code>syslog-ng</code> with data when <code>syslog_buffering</code> and/or <code>alarm</code> is active. When nonzero, the contents of the data buffer are sent to the <code>syslogng</code> every time a quantity of data equal to this parameter is collected. The <code>syslog</code> level for data buffering is hard coded to level five (notice) and facility <code>local[0+ conf.DB_facility]</code> . The file <code>/etc/syslog-ng/syslog-ng.conf</code> should be set accordingly for the <code>syslog-ng</code> to take some action. Example value: 0.
<i>all.syslog_buffering</i>	When nonzero, the contents of the data buffer are sent to the <code>syslog-ng</code> every time a quantity of data equal to this parameter is collected. The <code>syslog</code> message is sent to <code>syslog-ng</code> with NOTICE level and <code>LOCAL[0+conf.DB_facility]</code> facility.

Chapter 3 - Additional Features

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 TS.

In your browser's address field type:

`<Console Access Server's IP address>`

Step 2: Log in.

Enter `root` as the username and `tslinux` as the password. This will take you to the Configuration and Administration Menu Page.

Step 3: Click Syslog on the Configuration section.

Select the Syslog link. The following page will appear, giving information for configuring syslog:

Chapter 3 - Additional Features

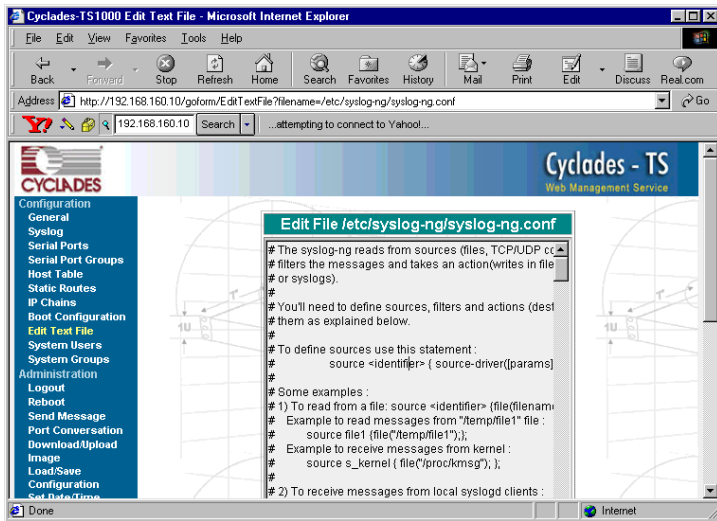


Figure 34: Syslog page 1

Step 4: Click the Edit Text File link on the Link Panel.
Enter the filename and begin editing the file.

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
```

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

Chapter 3 - Additional Features

Screen 2:

(Note: Screen 2 has the same instruction set preceding the parameters as seen in the section for Access Method. The instructions have been omitted for brevity's sake.)

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

Chapter 3 - Additional Features

Screen 3

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

Your current configuration parameters are:
(The ones with the '#' means it's not activated.)

```
conf.facility : 7
conf.DB_facility : 0
```

Are these configuration(s) all correct (Y)es or (N)o [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 4.

Screen 4:

```
*****
***** 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] :

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 *****  
*****
```

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]

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:

Chapter 3 - Additional Features

<i>time_reopen(n)</i>	The time to wait before a dead connection is reestablished.
<i>time_reap(n)</i>	The time to wait before an idle destination file is closed.
<i>sync_freq(n)</i>	The number of lines buffered before written to file. (The file is synced when this number of messages has been written to it.)
<i>mark_freq(n)</i>	The number of seconds between two MARKS lines.
<i>log_fifo_size(n)</i>	The number of lines fitting to the output queue.
<i>chain_hostname</i> <i>(yes/no)</i> or <i>long_hostname</i> <i>(yes/no)</i>	Enable/disable the chained hostname format.
<i>use_time_rcvd</i> <i>(yes/no)</i>	Use the time a message is received instead of the one specified in the message.
<i>use_dns (yes/no)</i>	Enable or disable DNS usage. syslog-ng blocks on DNS queries, so enabling DNS may lead to a Denial of Service attack.
<i>gc_idle_threshold(n)</i>	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.
<i>gc_busy_threshold(n)</i>	Sets the threshold value for the garbage collector. When syslog-ng is busy, GC phase starts.
<i>create_dirs(yes/no)</i>	Enable the creation of new directories.
<i>owner(name)</i>	Set the owner of the created file to the one specified. Default: root.
<i>group(name)</i>	Set the group of the created file to the one specified. Default: root.
<i>perm(mask)</i>	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:

<i>identifier</i>	Has to uniquely identify this given source.
<i>source-driver</i>	Is a method of getting a given message.
<i>params</i>	Each source-driver may take parameters. Some of them are required, some of them are optional.

The following source-drivers are available:

<i>a) internal()</i>	Messages are generated internally in syslog-ng.
<i>b) unix-stream (filename [options])</i>	They open the given AF_UNIX socket, and start listening for messages. Options: owner(name), group(name), perm(mask) are equal global options
<i>and</i>	
<i>unix-dgram (filename [options])</i>	<i>keep-alive(yes/no)</i> - Selects whether to keep connections opened when syslog-ng is restarted. Can be used only with <i>unix_stream</i> . Default: yes <i>max-connections(n)</i> - Limits the number of simultaneously opened connections. Can be used only with <i>unix_stream</i> . Default: 10.

Chapter 3 - Additional Features

- c) tcp(*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.
- and* 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.
- udp(*options*)*
- 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 sys1 {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))};
```

Example to listen to messages from one client (IP address=10.0.0.1) on UDP port 999:

Chapter 3 - Additional Features

```
source s_udp_10 { udp(ip(10.0.0.1) port(999)); };
```

Task 3: Define filters.

To define filters use this statement:

```
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:

```
filter f_facilty { facility(<facility name>); };
```

Examples:

Chapter 3 - Additional Features

```
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:

<i>identifier</i>	Has to uniquely identify this given destination.
<i>destination driver</i>	Is a method of outputting a given message.
<i>params</i>	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.

Chapter 3 - Additional Features

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.

Chapter 3 - Additional Features

f) *program* (<program name and arguments>)

This driver fork()'s executes the given program with the arguments and sends messages down to the stdin of the child.

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:

<i>-t <name>[,<name>]</i>	To address
<i>[-c <name>[,<name>]]</i>	CC address
<i>[-b <name>[,<name>]]</i>	Bcc address
<i>[-r <name>[,<name>]]</i>	Reply-to address
<i>-f <name></i>	From address
<i>-s \<i>"<text>"</i></i>	Subject
<i>-m \<i>"<text message>"</i></i>	Message
<i>-h <IP address or name></i>	SMTP server
<i>[-p <port>]</i>	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).

Chapter 3 - Additional Features

<code>\$HOST</code>	The name of the source host.
<code>\$FULLHOST</code>	The name of the source host and the source driver. Format: <code><source>@<hostname></code>
<code>\$MSG</code> or <code>\$MESSAGE</code>	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 host-name of this TS and the message that was received from the source.

```
destination d_maill {
    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 {
    pipe('/dev/cyc_alarm'
```

Chapter 3 - Additional Features

```
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

<snmptrapd 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/cyc_alarm"  
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'\" ");  
};
```

Chapter 3 - Additional Features

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.)

```
log { source(S1); source(S2); ...  
filter(F1);filter(F2);...  
destination(D1); destination(D2);...  
};
```


Chapter 3 - Additional Features

where :

<i>Sx</i>	Identifier of the sources defined before.
<i>Fx</i>	Identifier of the filters defined before.
<i>Dx</i>	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);};
```

Chapter 3 - Additional Features

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); };
```

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\n\  
Welcome to terminal server %h port S%p \n\  
\r\n
```

Configuration for CAS, TS, and Dial-in Access

Browser Method

Step 1: Point your browser to the TS.

In the address field of your browser type:

```
<Console Access Server's IP address>
```

Step 2: Log in.

Log in as root, pwd is tslinux. 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: 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: Click on Administration > Restart Processes > signal_ras hup.

The new configuration is now running.

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.

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

Screen 2:

(Note: Screens 2 has the same instruction set preceding the parameters as seen in the section for Access Method. The instructions have been omitted for brevity's sake.)

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

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\
Welcome to terminal server %h port S%p \n\
\r\n
```

ALL.PROMPT - This text defines the format of the login prompt.

```
all.prompt[%h login:] :
```

Screen 3:

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

Your current configuration parameters are:
(The ones with the '#' means it's not activated.)

Chapter 3 - Additional Features

```
all.issue : \r\n\  
Welcome to terminal server %h port S%p \n\  
\r\n
```

```
all.prompt : %h login:
```

```
Are these configuration(s) all correct (Y)es or (N)o [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 4, typing 'q' leads to Screen 5.

Screen 4:

```
*****  
***** 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 5.

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 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] :

Screen 6:

```
*****
***** 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]

Chapter 3 - Additional Features

Time Zone

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:

```
std offset
```

The *std* string specifies the name of the time zone and must be three or more alphabetic characters. The offset string immediately follows *std* and specifies the time value to be added to the local time to get *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:

```
std offset dst [offset],start[/time],end[/time]
```

There are no spaces in the specification. The initial *std* and *offset* specify the Standard Time zone, as described above. The *dst* string and *offset* specify the name and offset for the corresponding daylight savings time zone. If the *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:

- Jn* This specifies the Julian day, with *n* being between 1 and 365. February 29 is never counted even in leap years.
- n* This specifies the Julian day, with *n* being between 1 and 365. February 29 is counted in leap years.
- 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.

Chapter 3 - Additional Features

In the example below:

```
GST+7DST+6M4.1.0/14:30.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 [MMDDhhmm[[CC]YY]
^ ^ ^ ^ ^ ^
^ ^ ^ ^ ^ year
^ ^ ^ ^ century
^ ^ ^ minute
^ ^ hour
^ day
month
```

For example:

```
date 101014452002
```

produces:

```
Thu Oct 10 14:45:00 DST 2002
```

The DST is because it was specified in /etc/TIMEZONE.

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 pre-defined, 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.

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.
- /mnt*** Contains information about mounted disks.
- /opt*** Location where packages not supplied with the operating system are stored.

Appendix A - New User Background Information

- /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.

- | | |
|--|---|
| <i>cp file_name destination</i> | Copies the file indicated by <i>file_name</i> to the path indicated by <i>destination</i> . |
| a) <i>cp text.txt /tmp</i> | a) Copies the file <i>text.txt</i> in the current directory to the <i>tmp</i> directory. |
| b) <i>cp /chap/robo.php ./excess.php</i> | b) Copies the file <i>robo.php</i> in the <i>chap</i> directory to the current directory and renames the copy <i>excess.php</i> . |
| <i>rm file_name</i> | Removes the file indicated by <i>file_name</i> . |
| <i>mv file_name destination</i> | Moves the file indicated by <i>file_name</i> to the path indicated by <i>destination</i> . |
| <i>mkdir directory_name</i> | Creates a directory named <i>directory_name</i> . |
| a) <i>mkdir spot</i> | a) creates the directory <i>spot</i> in the current directory. |
| b) <i>mkdir /tmp/snuggles</i> | b) creates the directory <i>snuggles</i> in the directory <i>tmp</i> . |
| <i>rmdir directory_name</i> | Removes the directory indicated by <i>directory_name</i> . |

Appendix A - New User Background Information

Other commands allow the user to change directories and see the contents of a directory.

<i>pwd</i>	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: <code>/home/<username></code>
<code>ls [options] directory_name</code>	Lists the files and directories within <code>directory_name</code> . Some useful options are <code>-l</code> for more detailed output and <code>-a</code> which shows hidden system files.
<code>cd directory_name</code>	Changes the directory to the one specified.
<code>cat file_name</code>	Prints the contents of <code>file_name</code> 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.

Appendix A - New User Background Information

Table 13: vi modes

Mode	What is done there	How to get there
Command mode	Navigation within the open file.	Press the <ESC> key.
Editing mode	Text editing.	See list of editing commands below.
Line mode	File saving, opening, e\tc. Exiting from vi.	From the command mode, type ":" (colon).

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 14: vi navigation commands

<i>h</i>	Moves the cursor to the left (left arrow).
<i>j</i>	Moves the cursor to the next line (down arrow).
<i>k</i>	Moves the cursor to the previous line (up arrow).
<i>l</i>	Moves the cursor to the right (right arrow).

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).

Table 15: vi file modification commands

<i>i</i>	Inserts text before the cursor position (everything to the right of the cursor is shifted right).
<i>o</i>	Creates a new line below the current line and insert text (all lines are shifted down).
<i>dd</i>	Removes the entire current line.
<i>x</i>	Deletes the letter at the cursor position.

Appendix A - New User Background Information

After you have finished modifying a file, enter line mode (by typing “:” from command mode) and use one of the following commands:

Table 16: vi line mode commands

w	Saves the file (w is for write).
wq	Saves and closes the file (q is for quit).
q!	Closes the file without saving.
w <i>file</i>	Saves the file with the name <i><file></i> .
e <i>file</i>	Opens the file named <i><file></i> .

The Routing 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:

```
route [add|del] [-net|-host] target netmask nt_msk [gw gt_way]
interf
```

Appendix A - New User Background Information

<i>[add/del]</i>	One of these tags must be present. Routes can be either added or deleted.
<i>[-net/-host]</i>	Net is for routes to a network and -host is for routes to a single host.
<i>target</i>	Target is the IP address of the destination host or network.
<i>netmask</i> <i>nt_msk</i>	The tag <i>netmask</i> and <i>nt_mask</i> are necessary only when subnetting is used, otherwise, a mask appropriate to the target is assumed. <i>nt_msk</i> must be specified in dot notation.
<i>gw gt_way</i>	Specifies a gateway, when applicable. <i>gt_way</i> is the IP address or hostname of the gateway.
<i>interf</i>	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*.

Appendix A - New User Background Information

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
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 -l 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)
```

Appendix A - New User Background Information

```
ssh -t -l 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 -> 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
```

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/ssh_config` the parameters:

```
Host *  
  
    RhostsAuthentication yes  
  
    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).

Appendix A - New User Background Information



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 TS/`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>`



Note: "client_hostname" should be the DNS name. To access the serial port, the TS must be configured for local authentication. No root user should be used as username.

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>`.

Appendix A - New User Background Information

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.

The Process Table

The process table shows which processes are running. Type `ps -a` to see a table similar to that below.

Table 17: Process table

PID	UID	State	Command
1	root	S	/sbin/inetd
31	root	S	/sbin/sshd
32	root	S	/sbin/cy_ras

Appendix A - New User Background Information

Table 17: Process table

PID	UID	State	Command
36	root	S	/sbin/cy_wdt_led wdt led
154	root	R	/ps -a

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`.

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`:

```
> ts_menu -h
```

```
USAGE: ts_menu options
```

```
-p : Display Ethernet Ip and Tcp port
```

```
-i : Display local Ip assigned to the serial port
```

```
-u <name> : Username to be used in ssh/telnet command
```

```
-U : Allows choosing of different usernames for different ports
```

```
-h : print this help message
```

Appendix A - New User Background Information

```
> 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:
```

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.

Appendix A - New User Background Information

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 B - Cabling, Hardware, & Electrical

General Hardware Specifications

The power requirements, environmental conditions and physical specifications of the Cyclades-TS are listed below.

Table 18: Cyclades-TS power requirements

Power Specifications						
	TS100	TS400	TS800	TS1000	TS2000	TS3000
Input Voltage Range	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)	External Universal Input Desktop Power Supply (100-240VAC auto-range input, 5VDC output)	External Universal Input Desktop Power Supply (100-240VAC auto-range input, 5VDC output)	Internal 100-240VAC autorange (-48VDC option available)	Internal 100-240VAC autorange (-48VDC option available)	Internal 100-240VAC autorange
Input Frequency Range	50/60H	50/60H	50/60H	50/60H	50/60H	50/60H
Power @120VAC	5 W max	5 W max	6 W max	22 W max	26 W max	11 W max
Power @220 VAC	6 W max	6 W max	8 W max	28 W max	37 W max	17 W max

Table 19: Cyclades-TS environmental conditions

Environmental Information						
	TS100	TS400	TS800	TS1000	TS2000	TS3000
Operating Temperature	50F to 112F (10°C to 50°C)	50F to 112F (10°C to 50°C)	50F to 112F (10°C to 50°C)	50F to 112F (10°C to 50°C)	50F to 112F (10°C to 50°C)	50F to 112F (10°C to 50°C)

Appendix B - Cabling, Hardware, & Electrical

Table 19: Cyclades-TS environmental conditions

Environmental Information						
Relative Humidity	10 - 90%, non-condensing	10 - 90%, non-condensing	10 - 90%, non-condensing	10 - 90%, non-condensing	10 - 90%, non-condensing	10 - 90%, non-condensing

Table 21: Cyclades-TS physical specifications

Physical Information						
	TS100	TS400	TS800	TS1000	TS2000	TS3000
External Dimensions	2.76 x 3.35 in. x 1.18 in.	8.5 in. x 4.75 in. x 1 in.	8.5 in. x 4.75 in. x 1 in.	17 in. x 8.5 in. x 1.75 in.	17 in. x 8.5 in. x 1.75 in.	17 in. x 8.5 in. x 1.75 in.
Weight	0.3 lb.	1.5 lb.	1.6 lb.	6 lb.	6.2 lb.	8 lb.

Table 22: Cyclades-TS safety specifications

Safety Information						
	TS100	TS400	TS800	TS1000	TS2000	TS3000
Approvals	FCC and CE, Class A					

This 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-TS100 model only.

Appendix B - Cabling, Hardware, & Electrical

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:

<i>Receive Data (RxD) and Transmit Data (TxD)</i>	The actual data signals
<i>Signal Ground (Gnd)</i>	Electrical reference for both ends
<i>Data Terminal Ready (DTR)</i>	Indicates that the computer (DTE) is active
<i>Data Set Ready (DSR)</i>	Indicates that the modem (DCE) is active.
<i>Data Carrier Ready (DCD)</i>	Indicates that the connection over the communication line is active
<i>CTS (Clear to Send, an input)</i>	Flow control for data flowing from DTE to DCE
<i>RTS (Request to Send, an output)</i>	Flow control for data flowing from DCE to DTE

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

Appendix B - Cabling, Hardware, & Electrical

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.

Appendix B - Cabling, Hardware, & Electrical

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 24: Cables and their pin specifications

RS-232 Signal	Name/Function (Input/Output)	DB-25 pins (Standard)	DB-9 pins (Standard)	RJ-45 pins (Cyclades)
Chassis	Safety Ground	1	Shell	Shell
TxD	Transmit Data (O)	2	3	3
RxD	Receive Data (I)	3	2	6
DTR	Data Terminal Ready (O)	20	4	2
DSR	Data Set Ready (I)	6	6	8
DCD	Data Carrier Detect (I)	8	1	7
RTS	Request To Send (O)	4	7	1
CTS	Clear To Send (I)	5	8	5
Gnd	Signal Ground	7	5	4

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.

Appendix B - Cabling, Hardware, & Electrical

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 25: Which cable to use

To Connect To	Use Cable
DCE DB-25 Female (standard) <ul style="list-style-type: none">• Analog Modems• ISDN Terminal Adapters	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”).
DTE RJ-45 Cyclades (custom) <ul style="list-style-type: none">• All Cyclades Console Ports	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.
DTE DB-25 to DB-9 Cyclades (custom) <ul style="list-style-type: none">• For the Cyclades-TS100	Cable 3: DB-9 Female to DB-25 Female crossover. This connects the Cyclades-TS100 (serial port) to terminals, printers and other DTE RS-232 devices.

Appendix B - Cabling, Hardware, & Electrical

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.

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. After connecting the appropriate adapter to the RJ-45 straight-through cable, you will essentially have the cable shown in this picture.

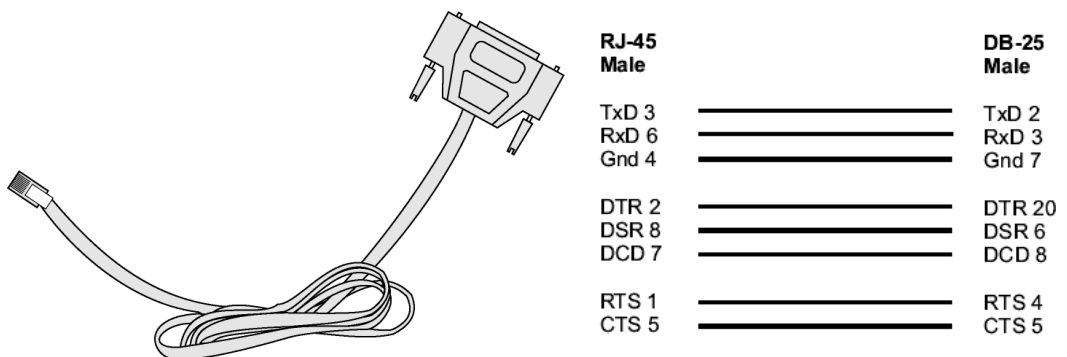


Figure 35: Cable 1 - Cyclades RJ-45 to DB-25 Male, straight-through

Appendix B - Cabling, Hardware, & Electrical

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. After connecting the appropriate adapter to the RJ-45 straight-through cable, you will essentially have the cable shown in this picture.

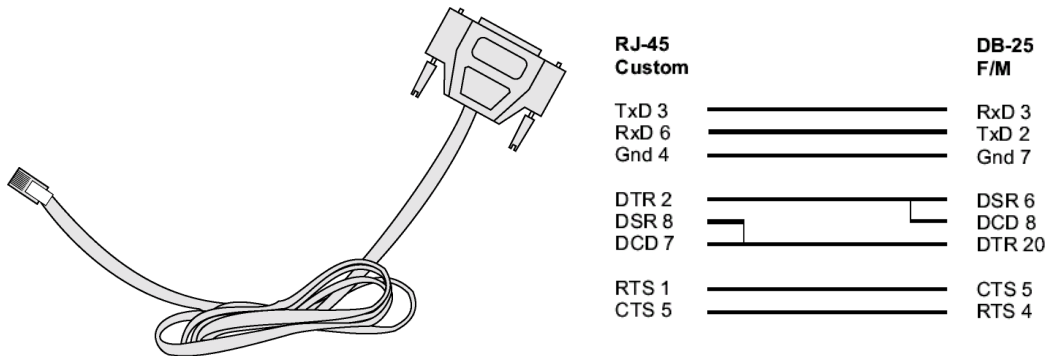


Figure 36: Cable 2 - Cyclades RJ-45 to DB-25 Female/Male, crossover

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. After connecting the appropriate adapter to the RJ-45 straight-through cable, you will essentially have the cable shown in this picture.

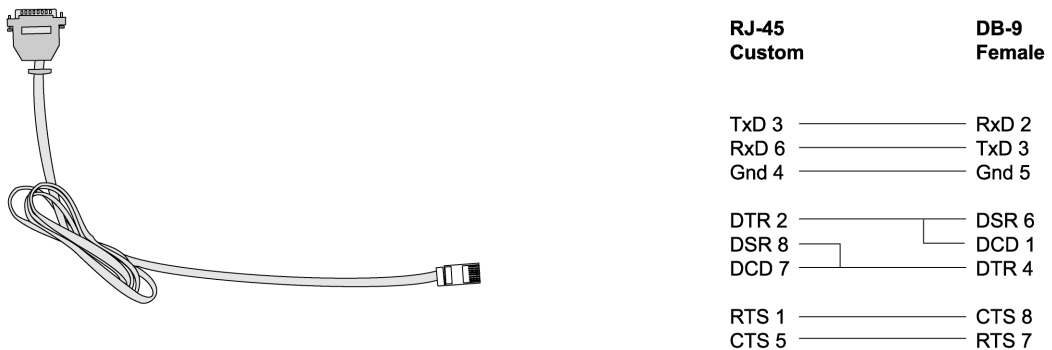


Figure 37: Cable 3 - Cyclades RJ-45 to DB-9 Female, crossover

Appendix B - Cabling, Hardware, & Electrical

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 (RJ45-to-DB9 or RJ45-to-DB25) you can create a crossover cable like the ones explained in Cable #2 or #3 for configuration or to connect to a server.

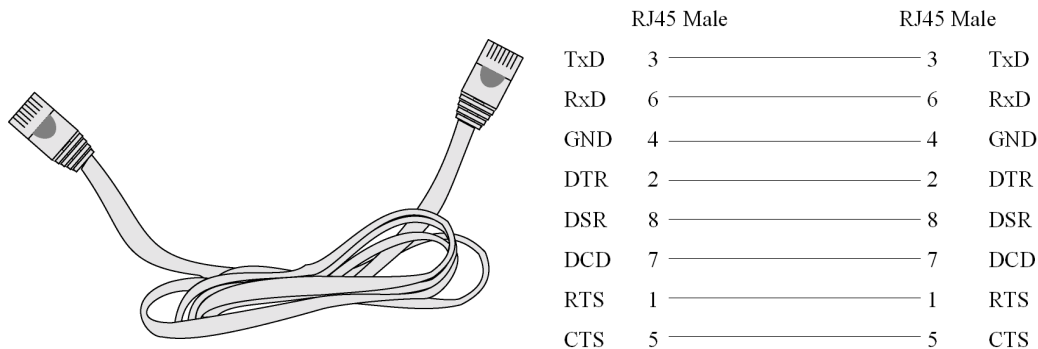


Figure 38: Cable 4 - Cyclades RJ-45 to Cyclades RJ-45, straight-through

Loop-Back Connector for Hardware Test

The use of the following DB-25 connector is explained in the Troubleshooting chapter.

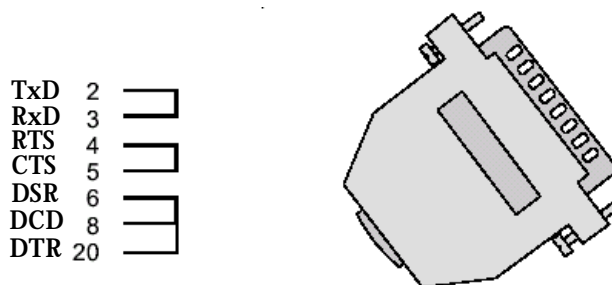


Figure 39: Loop-Back Connector

Appendix B - Cabling, Hardware, & Electrical

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.

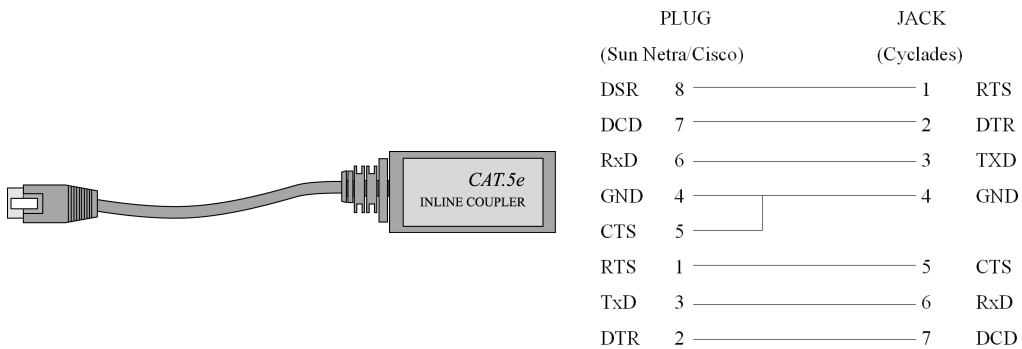


Figure 40: Cyclades\Sun Netra Adapter

Appendix B - Cabling, Hardware, & Electrical

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.

RJ-45 Female to DB-25 Male Adapter

The following adapter may be necessary.

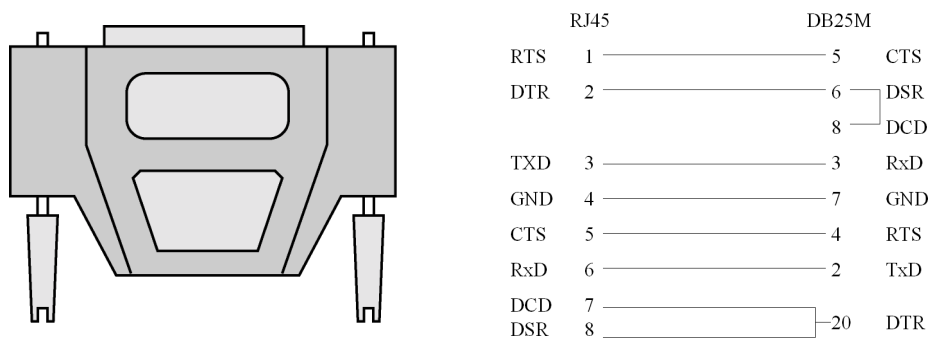


Figure 41: RJ-45 Female to DB-25 Male Adapter

RJ-45 Female to DB-25 Female Adapter

The following adapter may be necessary.

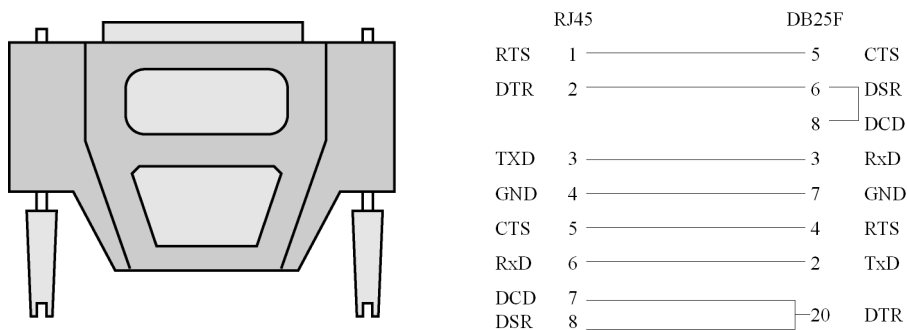


Figure 42: RJ-45 Female to DB-25 Female Adapter

Appendix B - Cabling, Hardware, & Electrical

RJ-45 Female to DB-9 Male Adapter

The following adapter may be necessary.

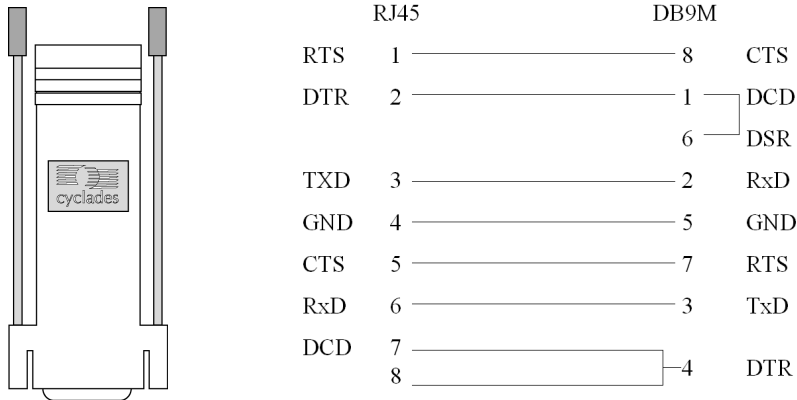


Figure 43: RJ-45 Female to DB-9 Male Adapter

RJ-45 Female to DB-9 Female Adapter

The following adapter may be necessary.

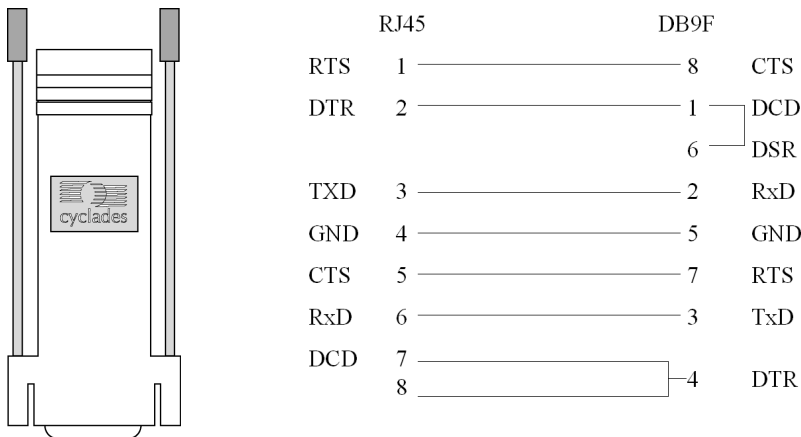


Figure 44: RJ-45 Female to DB-9 Female Adapter

Appendix B - Cabling, Hardware, & Electrical

DB-25 Male to DB-9 Female Adapter

The following adapter may be necessary.

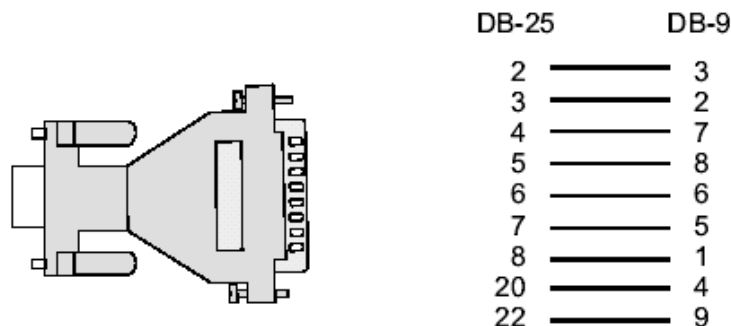


Figure 45: DB-25 Male to DB-9 Female Adapter

TS100-only cabling information

The RS-485 Standard

The RS-485 is another standard for serial communication and is available only in the Cyclades-TS100. 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.

TS100 Connectors

Although the RS-485 can be provided in different kinds of connectors, the Cyclades-TS100 uses a 9-pin D-shaped connector (DB-9) and a block connector with the pin assignment described below.

Appendix B - Cabling, Hardware, & Electrical

Table 28: TS100 Connector pin assignment

RS-485 Signal	Name/Function	DB-9 pins	Block connector pins
Chassis	Safety Ground		1
TXD-	Transmit Data - (A)	7	2
TXD+	Transmit Data + (B)	3	3
RXD+	Receive Data + (B)	2	4
RXD-	Receive Data - (A)	8	5
Chassis	Safety Ground		6

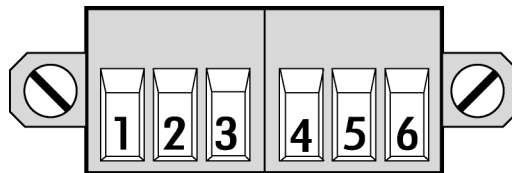


Figure 46: Pin assignment control

Notice that if the Cyclades-TS100 is configured to use RS-485, the RS-485 signals will be available in both DB-9 and block connector. 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 Cyclades-TS100 (serial port) DTE RS-485 devices with half duplex communication.

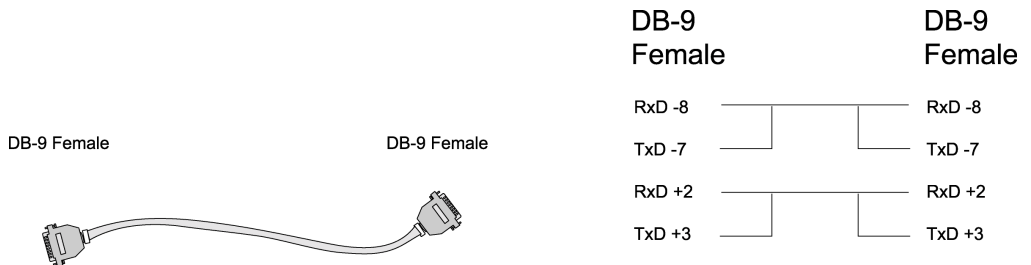


Figure 47: Cable 1 for TS100 - DB-9 Female to DB-9 Female, Crossover half duplex

Cable #2: DB-9 Female to DB-9 Female, Crossover full duplex

Application: It connects the Cyclades-TS100 (serial port) to DTE RS-485 devices with full duplex communication.

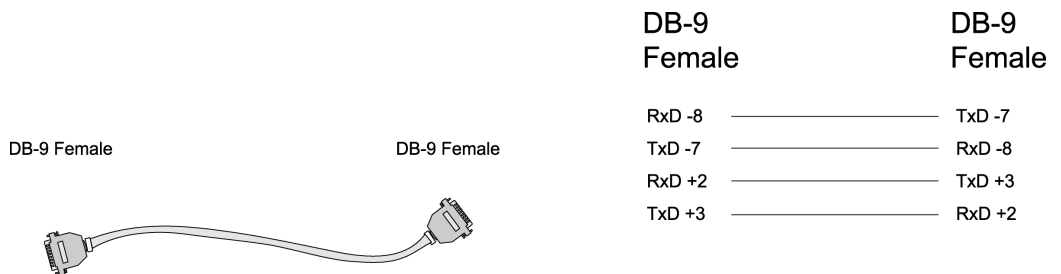


Figure 48: Cable 2 for TS100 - DB-9 Female to DB-9 Female, Crossover full duplex

Appendix B - Cabling, Hardware, & Electrical

Cable #3: Block Connector to Block Connector, Crossover half duplex

Application: It connects the Cyclades-TS100 (serial port) to DTE RS-485 devices with half duplex communication.

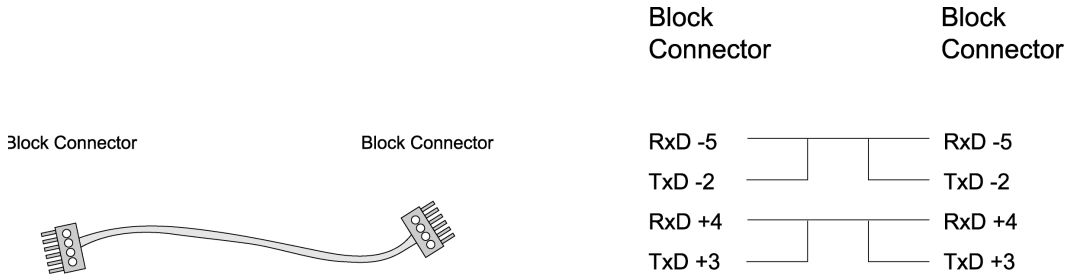


Figure 49: Cable 2 for TS100 - Block Connector to Block Connector, Crossover half duplex

Cable #4: Block Connector to Block Connector, Crossover full duplex

Application: It connects the Cyclades-TS100 (serial port) to DTE RS-485 devices with full duplex communication.

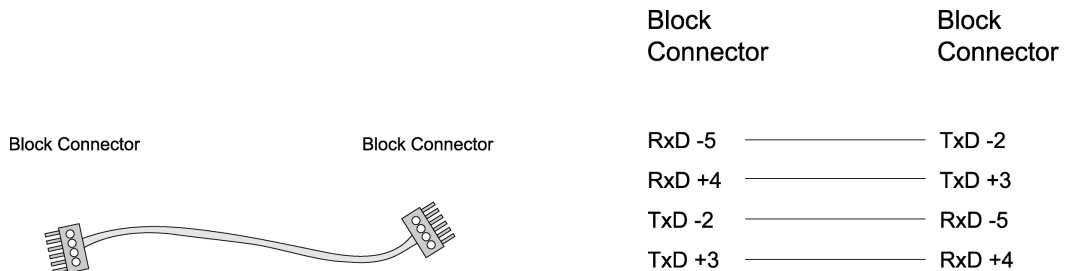


Figure 50: Cable 4 for TS100 - Block Connector to Block Connector, Crossover full duplex

Appendix B - Cabling, Hardware, & Electrical

This page has been left intentionally blank.

Appendix C - The pslave Configuration File

Introduction

This chapter begins with the complete table for all parameters and their descriptions. The `pslave.conf` file with all possible parameters and their descriptions follows. 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 Parameters

You can configure additional CAS features with the parameters given on the following tables. (The [Figure 1: Console Access Server diagram](#) is used as an example in some parameters. Other values are default values.):

Table 29: Parameters Common to CAS, TS, & Dial-in Access

Parameter	Description	Value for this Example
<code>conf.eth_ip</code>	Configured in Task 4: Edit the pslave.conf file in Chapter 2 - Installation and Configuration . This is the IP address of the Ethernet interface. This parameter, along with the next two, is used by the <code>cy_ras</code> program to OVERWRITE the file <code>/etc/network/ifcfg_eth0</code> as soon as the command “ <code>signal_ras hup</code> ” is executed. The file <code>/etc/network/ifcfg_eth0</code> should not be edited by the user unless the <code>cy_ras</code> configuration is not going to be used.	200.200.200.1
<code>conf.eth_mask</code>	The mask for the Ethernet network.	255.255.255.0
<code>conf.eth_mtu</code>	The Maximum Transmission Unit size, which determines whether or not packets should be broken up.	1500

Appendix C - The pslave Configuration File

Table 29: Parameters Common to CAS, TS, & Dial-in Access

Parameter	Description	Value for this Example
conf.lockdir	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.	/var/lock
all.speed	The speed for all ports.	9600
all.datasize	The data size for all ports.	8
all.stopbits	The number of stop bits for all ports.	1
all.parity	The parity for all ports.	none
all.authtype	Configured in Task 4: Edit the pslave.conf file in Chapter 2 - Installation and Configuration .	radius
all.authhost1	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.	200.200.200.2
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.	200.200.200.2

Appendix C - The pslave Configuration File

Table 29: Parameters Common to CAS, TS, & Dial-in Access

Parameter	Description	Value for this Example
all.authtype	<p>Type of authentication used. There are several authentication type options:</p> <ul style="list-style-type: none">• <i>local</i> (authentication is performed using the /etc/passwd file)• <i>radius</i> (authentication is performed using a Radius authentication server)• <i>TacacsPlus</i> (authentication is performed using a TacacsPlus authentication server)• <i>none</i>• <i>local/radius</i> (authentication is performed locally first, switching to Radius if unsuccessful)• <i>radius/local</i> (the opposite of the previous option),• <i>RadiusDownLocal</i> (local authentication is tried only when the Radius server is down)• <i>local/TacacsPlus</i> (authentication is performed locally first, switching to TacacsPlus if unsuccessful)• <i>ldap</i> (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) <p>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.</p>	local

Appendix C - The pslave Configuration File

Table 29: Parameters Common to CAS, TS, & Dial-in Access

Parameter	Description	Value for this Example
all.radtimeout	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.	3
all.radretries	Defines the number of times each Radius/TacacsPlus server is tried before another is contacted. The default, if not configured, is 5.	5
all.secret	This is the shared secret necessary for communication between the Cyclades-TS and the Radius/TacacsPlus servers.	rad-secret
all.flow	This sets the flow control to hardware, software, or none.	hard
all.protocol	The default CAS setup was explained in Chapter 2, Task 4: Edit the pslave.conf file . The TS configuration settings are in Table 31, “TS Parameters,” on page 258 . The Dial-in configuration settings are in Table 32, “Dial-in configuration Parameters,” on page 259 .	socket_server
s1.tty	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.	ttyS1

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.

Appendix C - The pslave Configuration File

Table 30: Mostly CAS-specific Parameters

Parameter	Description	Value for this Example
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 <i>/var/run/DB</i> . 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 <i>all.data_buffering</i> , 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.).	commented
conf.facility	This value (0-7) is the Local facility sent to the syslog. The file <i>/etc/syslogng/syslog-ng.conf</i> contains a mapping between the facility number and the action (see more in Syslog in Chapter 3 - Additional Features).	7
conf.DB_facility	This value (0-7) is the Local facility sent to the syslog with the data when <i>syslog_buffering</i> is active. The file <i>/etc/syslog-ng/syslog-ng.conf</i> contains a mapping between the facility number and the action (see more on Syslog in Chapter 3).	0
conf.group	Used to group users to simplify configuration of the parameter <i>all.users</i> later on. This parameter can be used to define more than one group.	group_name: user1, user2

Appendix C - The pslave Configuration File

Table 30: Mostly CAS-specific Parameters

Parameter	Description	Value for this Example
all.DTR_reset	Valid only for the CAS configuration. This value specifies how long (in milliseconds) a DTR signal will be turned off before it is turned back on again. If set to 0, this parameter will NOT be active. This may be dangerous if a user were to connect to a port that a previous user was on but had lost the session after a timeout. The user may directly connect into the previous user's shell. A minimum of 100ms is required otherwise it is assumed.	100
all.break_sequence	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.	~break
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.	0
all.modbus_smode	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.	commented

Appendix C - The pslave Configuration File

Table 30: Mostly CAS-specific Parameters

Parameter	Description	Value for this Example
all.issue	<p>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.</p> <p><i>Value for this Example:</i></p> <pre>\r\n\ Welcome to terminal server %h port S%p \r\n\</pre>	See Description column
all.prompt	<p>This text defines the format of the login prompt. Expansion characters can be used here.</p>	%h login:
all.ipno	<p>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.</p>	192.168.1.10 1+
all.poll_interval	<p>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.</p>	0

Appendix C - The pslave Configuration File

Table 30: Mostly CAS-specific Parameters

Parameter	Description	Value for this Example
all.socket_port	<p>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<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.</p> <p>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.</p>	7001+

Appendix C - The pslave Configuration File

Table 30: Mostly CAS-specific Parameters

Parameter	Description	Value for this Example
all.data_buffering	<p>A non zero value activates data buffering (local or remote, according to what was configured in the parameter conf.nfs_data_buffering see Data Buffering in Chapter 3). 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.). <i>Size is in bytes not kilobytes</i>. See Data Buffering for details.</p>	0

Appendix C - The pslave Configuration File

Table 30: Mostly CAS-specific Parameters

Parameter	Description	Value for this Example
all.DB_mode	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<n>.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.f low or s<n>.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 (dont_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<n>.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.	cir
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.	0

Appendix C - The pslave Configuration File

Table 30: Mostly CAS-specific Parameters

Parameter	Description	Value for this Example
<code>all.syslog_buffering</code>	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 <code>local[0+conf.DB_facility]</code> . The file <code>/etc/syslog-ng/syslog-ng.conf</code> should be set accordingly for the syslog-ng to take some action. (See Syslog-ng Configuration to use with Syslog Buffering Feature.)	0
<code>all.dont_show_DBmenu</code>	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.	1
<code>all.alarm</code>	When non zero, all data received from the port are captured and sent to syslog-ng with level INFO and <code>local[0+conf.DB_facility]facility</code> . The <code>syslogng.conf</code> 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).	0

Appendix C - The pslave Configuration File

Table 30: Mostly CAS-specific Parameters

Parameter	Description	Value for this Example
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.) 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.	! joe, mark, 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): <i>in</i> shows data written to the port, <i>out</i> shows data received from the port, and <i>i/o</i> shows both streams. 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.	out
all.admin_users	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 auth-type must not be none. User groups (defined with the parameter conf.group) can be used in combination with user names in the parameter list.	peter, john, user_group

Appendix C - The pslave Configuration File

Table 30: Mostly CAS-specific Parameters

Parameter	Description	Value for this Example
<code>all.multiple_sessions</code>	If it is configured as "no" 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 and/or write permission. Please see Session Sniffing in Chapter 3 for details.	no
<code>all.escape_char</code>	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 '^'. This parameter is only valid when the port protocol is <code>socket_server</code> or <code>socket_ssh</code> . Default value is '^z'.	^z
<code>all.tx_interval</code>	Valid for protocols <code>socket_server</code> and <code>raw_data</code> . 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.	100
<code>all.idletimeout</code>	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.	0

Appendix C - The pslave Configuration File

Table 30: Mostly CAS-specific Parameters

Parameter	Description	Value for this Example
all.sttyCmd	<p>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 :</p> <p><i>-igncr</i> This tells the terminal not to ignore the carriage-return on input,</p> <p><i>-onlcr</i> Do not map newline character to a carriage return or newline character sequence on output,</p> <p><i>opost</i> Post-process output,</p> <p><i>-icrnl</i> Do not map carriage-return to a newline character on input.</p> <pre>all.sttyCmd -igncr -onlcr opost -icrnl</pre>	commented
s1.serverfarm	Alias name given to the server connected to the serial port. Server_connected.	serial1
s2.tty	See the s1.tty entry in the following table.	ttyS2
s8.tty	See the s1.tty entry in the following table.	ttyS8

CAS Setup Scenario

As shown in [Figure 1: Console Access Server diagram](#), our “CAS with local authentication” scenario has either telnet or ssh (a secure shell session) being used.

After configuring desired additional parameters, execute the command `signal_ras hup` to activate the changes. At this point, the configuration should be tested. A step-by-step check list follows:

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>`.

Appendix C - The pslave Configuration File

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 [Task 8: Reboot the Cyclades-TS](#) listed in [Chapter 2 - Installation and Configuration](#).

Appendix C - The pslave Configuration File



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.

TS Parameters

The following parameters are unique to a TS setup except where indicated.

Table 31: TS Parameters

Parameter	Description	Value for this Example
conf.telnet	Location of the telnet utility	/bin/telnet
conf.ssh	Location of the ssh utility.	/bin/ssh
conf.locallogins	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.	0
all.host	The IP address of the host to which the terminals will connect.	200.200.200.3
all.term	This parameter defines the terminal type assumed when performing rlogin or telnet to other hosts.	vt100
all.userauto	Username used when connected to a UNIX server from the user's serial terminal.	

Appendix C - The pslave Configuration File

Table 31: TS Parameters

Parameter	Description	Value for this Example
all.protocol (for TS)	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.	rlogin
all.issue (CAS and TS)	See description in CAS section.	
all.prompt (CAS and TS)	See description in CAS section.	
all.socket_port	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).	
s16.tty (TS)	See the s1.tty entry in the CAS section.	ttyS16

Dial-in Access Parameters

The following parameters are unique to a Dial-in setup except where indicated.

Table 32: Dial-in configuration Parameters

Parameter	Description	Value for this Example
conf.pppd	Location of the ppp daemon with Radius.	/usr/local/sbin/pppd
conf.facility (CAS and Dial-in)	See description in CAS section.	

Appendix C - The pslave Configuration File

Table 32: Dial-in configuration Parameters

Parameter	Description	Value for this Example
all.ipno (CAS and Dial-in)	See description in CAS section.	
all.initchat	Modem initialization string.	<pre>TIMEOUT 10 "" \d\ \dATZ \ OK\r\n-ATZ-OK\r\n "" \ "" ATMO OK\R\N "" \ TIMEOUT 3600 RING "" \ STATUS Incoming %p:I.HANDSHAKE "" ATA\ TIMEOUT 60 CONNECT@ "" \ STATUS Connected %p:I.HANDSHAKE</pre>
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).	<pre>%j novj \ proxyarp modem asyncmap 000A0000 \ noipx noccp login auth require-pap refusechap\ mtu %t mru %t \ cb-script /etc/portslave/cb_script \ plugin /usr/lib/libpsr.so</pre>

Appendix C - The pslave Configuration File

Table 32: Dial-in configuration Parameters

Parameter	Description	Value for this Example
all.pppopt	all.pppopt PPP options when user has already been authenticated.	<code>%i:%j novj \ proxyarp modem asyncmap 000A0000 \ noipx noccp mtu %t mru %t netmask%m \ idle %I maxconnect %T \ plugin /usr/lib/libpsr.so</code>
all.protocol	For the Dial-in configuration, the available protocols are PPP, SLIP and CSLIP.	<code>ppp</code>
s32.tty	See the s1.tty entry in the CAS section.	<code>ttyS32</code>

Appendix D - Linux-PAM

Introduction

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` (or a series of configuration files located in `/etc/pam.d/`) 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:

Appendix D - Linux-PAM

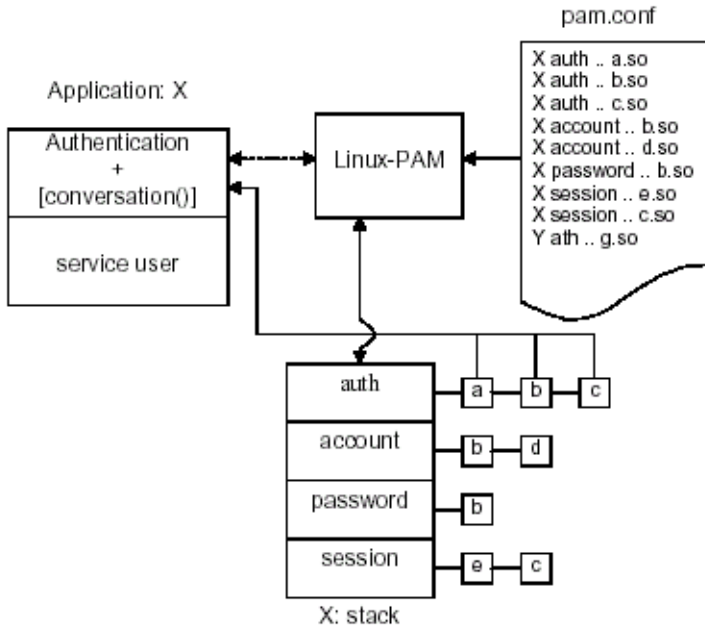


Figure 51: Data flow diagram of Linux-PAM

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.

Appendix D - Linux-PAM

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 one of two places: either the single system file `/etc/pam.conf` or the `/etc/pam.d/` directory. 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. The second (and more recently adopted) way of configuring Linux-PAM is via the contents of the `/etc/pam.d/` directory. After the meaning of the above tokens is explained, the method will be described.

Appendix D - Linux-PAM

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:

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.

Appendix D - Linux-PAM

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:

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 moduletype 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.

Appendix D - Linux-PAM

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.

Newest Syntax

The more elaborate (newer) syntax is much more specific and gives the administrator a great deal of control over how the user is authenticated. This form of the control flag is delimited with square brackets and consists of a series of value=action tokens:

```
[value1=action1 value2=action2 ...]
```

Here, value1 is one of the following return values: success; open_err; symbol_err; service_err; system_err; buf_err; perm_denied; auth_err; cred_insufficient; authinfo_unavail; user_unknown; maxtries; new_authtok_reqd; acct_expired; session_err; cred_unavail; cred_expired; cred_err; no_module_data; conv_err; authtok_err; authtok_recover_err; authtok_lock_busy; authtok_disable_aging; try_again; ignore; abort; authtok_expired; module_unknown; bad_item; and default. The last of these (default) can be used to set the action for those return values that are not explicitly defined.

The action can be a positive integer or one of the following tokens: ignore, ok, done, bad, die, and reset.

A positive integer When specified as the action, can be used to indicate that the next J modules of the current type will be skipped. In this way, the administrator can develop a moderately sophisticated stack of modules with a number of different paths of execution. Which path is taken can be determined by the reactions of individual modules.

Ignore When used with a stack of modules, the module's return status will not contribute to the return code the application obtains.

Appendix D - Linux-PAM

<i>Bad</i>	This action indicates that the return code should be thought of as indicative of the module failing. If this module is the first in the stack to fail, its status value will be used for that of the whole stack.
<i>Die</i>	Equivalent to <i>bad</i> with the side effect of terminating the module stack and PAM immediately returning to the application.
<i>OK</i>	This tells PAM that the administrator thinks this return code should contribute directly to the return code of the full stack of modules. In other words, if the former state of the stack would lead to a return of PAM_SUCCESS, the module's return code will override this value. Note: if the former state of the stack holds some value that is indicative of a module failure, this 'OK' value will not be used to override that value.
<i>Done</i>	Equivalent to OK with the side-effect of terminating the module stack and PAM immediately returning to the application.
<i>Reset</i>	Clear all memory of the state of the module stack and start again with the next stacked module.

Appendix D - 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:

<i>pam_access</i>	Provides logdaemon style login access control.
<i>pam_deny</i>	Deny access to all users.
<i>pam_env</i>	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.
<i>pam_filter</i>	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.)
<i>pam_group</i>	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.
<i>pam_issue</i>	This module presents the issue file (/etc/issue by default) when prompting for a username.
<i>pam_lastlog</i>	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.
<i>pam_limits</i>	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 below.

Appendix D - Linux-PAM

<i>pam_listfile</i>	The listfile module provides a way to deny or allow services based on an arbitrary file.
<i>pam_motd</i>	This module outputs the motd file (/etc/motd by default) upon successful login.
<i>pam_nologin</i>	Provides standard Unix nologin authentication.
<i>pam_permit</i>	This module should be used with extreme caution. Its action is to always permit access. It does nothing else.
<i>pam_radius</i>	Provides Radius server authentication and accounting.
<i>pam_rootok</i>	This module is for use in situations where the superuser wishes to gain access to a service without having to enter a password.
<i>pam_securetty</i>	Provides standard UNIX securetty checking.
<i>pam_time</i>	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.
<i>pam_tacplus</i>	Provides TacacsPlus Server authentication, authorization (account management), and accounting (session management).
<i>pam_unix</i>	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.
<i>pam_warn</i>	This module is principally for logging information about a proposed authentication or application to update a password.

Appendix D - Linux-PAM

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):

```
# 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).

Appendix D - Linux-PAM

- 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)`.

Appendix D - Linux-PAM

Directory-based Configuration

It is possible to configure libpam via the contents of the `/etc/pam.d/` directory. This is more flexible than using the single configuration file. In this case, the directory is filled with files—each of which has a filename equal to a service-name (in lower-case)—the personal configuration file for the named service. The Cyclades-TS Linux-PAM was compiled to use both `/etc/pam.d/` and `/etc/pam.conf` in sequence. In this mode, entries in `/etc/pam.d/` override those of `/etc/pam.conf`.

The syntax of each file in `/etc/pam.d/` is similar to that of the `/etc/pam.conf` file and is made up of lines of the following form:

```
module-type control-flag module-path arguments
```

The only difference between the two is that the service-name is not present. The service-name is of course the name of the given configuration file. For example, `/etc/pam.d/login` contains the configuration for the login service.

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
```

Appendix D - Linux-PAM

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; wake up! 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.

On a system that uses the `/etc/pam.d/` configuration, the corresponding default setup would be achieved with the following file:

```
#
# default configuration: /etc/pam.d/other
#
auth required pam_warn.so
auth required pam_deny.so
account required pam_deny.so
password required pam_warn.so
password required pam_deny.so
session required pam_deny.so
```


Appendix D - Linux-PAM

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.

```
# -----#
# /etc/pam.conf
#
#
#
# Last modified by Andrew G. Morgan <morgan@kernel.org>
#
# -----#
# $Id: pam.conf,v 1.2 2001/04/08 06:02:33 agmorgan Exp $
# -----#
# serv. module ctrl module [path] ...[args..]
```

Appendix D - Linux-PAM

```
#
# name type flag
# -----#
#
# The PAM configuration file for the 'tacplus' service
#
tacplus auth requisite pam_securetty.so
tacplus auth required pam_tacplus.so encrypt
tacplus account required pam_tacplus.so encrypt service=ppp proto-
col=lcp
tacplus session required pam_tacplus.so encrypt service=ppp proto-
col=lcp
#
# The PAM configuration file for the 'radius' service
#
radius auth requisite pam_securetty.so
radius auth required pam_radius_auth.so
radius account required pam_radius_auth.so
radius session required pam_radius_auth.so
#
# The PAM configuration file for the 'local' service
#
local auth requisite pam_securetty.so
local auth required pam_unix.so
```

Appendix D - Linux-PAM

```
local account required pam_unix.so
local password required pam_unix.so md5 use_authtok
local session required pam_unix.so
#
# The PAM configuration file for the 'remote' service
#
remote auth required pam_permit.so
remote account required pam_permit.so
remote password required pam_permit.so
remote session required pam_permit.so
#
# The PAM configuration file for the 'login' service
#
login auth requisite pam_securetty.so
login auth required pam_unix.so
login auth optional pam_group.so
login account requisite pam_time.so
login account required pam_unix.so
login password required pam_unix.so md5 use_authtok
login session required pam_unix.so
login session required pam_limits.so
#
# The PAM configuration file for the 'xsh' service
#
```

Appendix D - Linux-PAM

```
sshd auth requisite pam_securetty.so
sshd auth required pam_unix.so
sshd auth optional pam_group.so
sshd account requisite pam_time.so
sshd account required pam_unix.so
sshd password required pam_unix.so md5 use_authtok
sshd session required pam_unix.so
sshd session required pam_limits.so
#
# The PAM configuration file for the 'passwd' service
#
passwd password required pam_unix.so md5
#
# The PAM configuration file for the 'samba' service
#
samba auth required pam_unix.so
samba account required pam_unix.so
#
# The PAM configuration file for the 'su' service
#
su auth required pam_wheel.so
su auth sufficient pam_rootok.so
su auth required pam_unix.so
su account required pam_unix.so
```

Appendix D - Linux-PAM

```
su session required pam_unix.so
#
# Information for the PPPD process with the 'login' option.
#
ppp auth required pam_nologin.so
ppp auth required pam_unix.so
ppp account required pam_unix.so
ppp session required pam_unix.so
#
# The PAM configuration file for the 'other' service
#
other auth required pam_warn.so
other auth required pam_deny.so
other account required pam_deny.so
other password required pam_warn.so
other password required pam_deny.so
other session required pam_deny.so
```

Reference

The Linux-PAM System Administrators' Guide
Copyright (c) Andrew G. Morgan 1996-9. All rights reserved.
Email: morgan@linux.kernel.org

Appendix E - Customization and the CDK

Introduction

Everything related to the Cyclades-TS can be traced back to two files:

- /etc/rc.sysinit
- /etc/inittab

All Cyclades-TS application programs are started during boot by the init process. The related lines in the /etc/inittab file are listed below:

```
# System initialization.
::sysinit:/etc/rc.sysinit

# Single user shell

#console::respawn:/bin/sh < /dev/console > /dev/console 2> /dev/
console

ttyS0::respawn:/sbin/getty -p ttyS0 ansi
::respawn:/sbin/cy_wdt_led wdt led

# Cyclades RAS
::once:/sbin/cron
::once:/sbin/snmpd
::once:/sbin/cy_buffering
::once:/sbin/cy_ras
::once:/sbin/sshd -f /etc/ssh/sshd_config
::once:/sbin/ex_ntpclient
::once:/bin/webs
::once:/bin/syslog-ng
::once:/bin/cy_alarm
::wait:/sbin/fwset restore
```

Appendix E - Customization and the CDK

The Customization Process

To customize the Cyclades-TS, change these lines or add others. If the `/etc/inittab` file is changed, edit the `/etc/config_files` file and add a line containing only `"/etc/inittab"`. Save the file and exit the editor. Save the new configuration by executing `saveconf`. Then, the Cyclades-TS should be rebooted. This is necessary because the `init` program provided by Busybox--a tool that emulates `rm`, `cp`, etc., but uses much less space--does not support the option `q`.

The Cyclades Development Kit

Cyclades provides a development kit which allows changes to be made to the Cyclades-TS's software. However, Cyclades does not provide free technical support for systems modified in this way. Any changes are the responsibility of the user. The Cyclades Developer Kit (CDK) is available on the Cyclades Web site. Contact Tech Support to download the CDK.

Appendix F - 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 theTS as root.

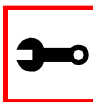
Provide the root password if requested.

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 F - 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. TheTS 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

```
cat /proc/version
```

to see the Linux kernel version.

Appendix F - 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, during the self test, press <Esc> after the Ethernet test.

Step 3: When the Watch Dog Timer prompt appears, press <Enter>.

Step 4: Choose the option Network Boot when asked.

Step 5: Enter the IP address of the Ethernet interface.

Step 6: Enter the IP address of the host where the new zImage file is located.

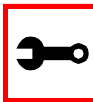
Step 7: Enter the file name of the zImage file on the host.

Step 8: 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 9: 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.



Note: Possible causes for the loss of flash memory may include: downloaded wrong zImage file, downloaded as ASCII instead of binary; problems with flash memory.

Appendix F - Upgrades and Troubleshooting

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 33: Files to be included in */etc/config_file* and the program to use

File	Program
<i>/etc/securetty</i>	telnet, login, su
<i>/etc/issue</i>	getty
<i>/etc/getty_ttyS0</i>	login (via console)
<i>/etc/hostname</i>	tcp
<i>/etc/hosts</i>	tcp
<i>/etc/host.conf</i>	tcp
<i>/etc/nsswitch.conf</i>	dns
<i>/etc/resolv.conf</i>	dns
<i>/etc/config_files</i>	saveconf
<i>/etc/passwd</i>	login, passwd, adduser...
<i>/etc/group</i>	login, passwd, adduser...
<i>/etc/ssh/ssh_host_key.pub</i>	sshd
<i>/etc/ssh/sshd_config</i>	sshd
<i>/etc/ssh/ssh_config</i>	ssh client
<i>/etc/ssh/ssh_host_key</i>	sshd (ssh1)
<i>/etc/ssh/ssh_host_key.pub</i>	sshd (ssh1)

Appendix F - Upgrades and Troubleshooting

Table 33: Files to be included in `/etc/config_file` and the program to use

File	Program
<code>/etc/ssh/ssh_host_dsa_key</code>	sshd (ssh2)
<code>/etc/ssh/ssh_host_dsa_key.pub</code>	sshd (ssh2)
<code>/etc/snmp/snmpd.conf</code>	snmpd
<code>/etc/portslave/pslave.conf</code>	cy_ras, portslave, TS configuration information
<code>/etc/network/ifcfg_eth0</code>	ifconfig eth0, cy_ras, rc.sysinit
<code>/etc/network/ifcfg*</code>	ifconfig, cy_ras, rc.sysinit
<code>/etc/network/ifcfg_lo ifconfig</code>	lo, cy_ras, rc.sysinit
<code>/var/run/radsession.id</code>	radinit, radius authentication process
<code>/home</code>	adduser, passwd
<code>/etc/network/st_routes</code>	ifconfig, cy_ras, rc.sysinit
<code>/etc/syslog-ng/syslog-ng.conf</code>	syslog-ng



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.



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.

Appendix F - Upgrades and Troubleshooting

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 TS100, 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 F - Upgrades and Troubleshooting

		<- Packets ->			<- Errors ->			
From	To	Sent	Received	Passes	Data	CTS	DCD	DSR
2	<-> 2	35	35	35	0	0	0	0
4	<-> 5	35	35	35	0	0	0	0
5	<-> 4	35	35	35	0	0	0	0

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.

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.

State	DTR	DCD	DSR	RTS	CTS
ON	X			X	
	↓			↓	
OFF		X	X		X

Figure 52: Initial test

Appendix F - 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.

State	DTR	DCD	DSR	RTS	CTS
ON	X	X	X	X	
	↓	↓	↓		
OFF					X

Figure 53: 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.

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.

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
```

Appendix F - Upgrades and Troubleshooting

```
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
```

For configuration problems, the user has two options:

Step 1: Edit the file(s) causing the problem with vi, then execute the commands:

```
saveconf
reboot
```

Step 2: Reset the configuration by executing the commands:

```
echo 0 > /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

Appendix F - Upgrades and Troubleshooting

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 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-TS100 console port

There is no dedicated console port available in the Cyclades-TS100. 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-TS100 off.

Step 2: Connect the Cyclades-TS100 to a terminal configured to work at 9600 bps, with 8 bits, no parity and 1 stop bit.

Appendix F - Upgrades and Troubleshooting

Step 3: Press and hold the ADM button and power on the Cyclades-TS100.

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-TS100 will 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-TS100 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]
Boot type ((B)ootp,(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]
```

Appendix F - Upgrades and Troubleshooting

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.

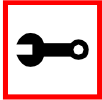
CPU LED

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 34: CPU LED Code Interpretation

Event	CPU LED Morse code
Normal Operation	S (short, short, short . . .)
Flash Memory Error - Code	L (long, long, long . . .)
Flash Memory Error - Configuration	S, L
Ethernet Error	S, S, L
No Interface Card Detected	S, S, S, L
Network Boot Error	S, S, S, S, L
Real-Time Clock Error	S, S, S, S, S, L

Appendix F - Upgrades and Troubleshooting



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 G - 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 35: Required information for the OpenSSL package

Parameter	Description
Country Name (2 letter code) [AU]:	The country code consisting of two letters.
State or Province Name (full name) [Some-State]:	Provide the full name (not the code) of the state.
Locality Name (e.g., city) []:	Enter the name of your city.
Organization Name (e.g., company) [Internet Widgits Ltd]:	Organization that you work for or want to obtain the certificate for.
Organizational Unit Name (e.g., section) []:	Department or section where you work.
Common Name (e.g., your name or your server's hostname) []:	Name of the machine where the certificate must be installed.

Appendix G - Certificate for HTTP Security

Table 35: Required information for the OpenSSL package

Parameter	Description
Email Address []:	Your email address or the administrator's email address.

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 G - Certificate for HTTP Security

Step E: Save the configuration in flash.

```
#saveconf
```

Step F: The certification will be effective in the next reboot.

Appendix H - 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.

Tested Environment

Table 36: Windows XP + JREv1.4.0_01 or 02

Internet Explorer 6.0	Success
Netscape 6/6.2.3	Success
Netscape 7.0	Success
Mozilla 1.1	Success

Table 37: Redhat 7.3 + JREv1.4.0_01 or 02

Netscape 7.0	Success
Mozilla 1.1	Success

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 H - 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 H - Connect to Serial Ports from Web

On Linux

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. If you have installed JRE, but the correct Java Plug-in is not shown, this may mean the browser is not locating the correct plug-in.

To fix this, go to the directory where your browser is installed. Then make a soft link from <netscape or mozilla>/plugins/. to the plug-in module in your JRE directory.

For example for Netscape:

```
ln -s <jre>/plugin/i386/ns600/libjavaplugin_oji.so <netscape>/plugins/.
```

where, <jre> is the path to your Java Runtime Environment (JRE) installation and <netscape> is the path to your Netscape installation. The plug-in for Mozilla should be the one under <jre>/plugin/i386/ns610/.... After creating the link, check again to see if your browser recognized the plug-in.

Step-by-Step Process

Step 1: Point your browser to the Console Server.

In the address field of your browser type the IP address of your Console Server.

<Console Server's IP address>

Step 2: Log in.

Log in as root, pwd is tslinux. This will take you to the Configuration and Administration page.

Appendix H - Connect to Serial Ports from Web

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.



Figure 54: 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 Submit button. This will take you to the Port Connection Page.

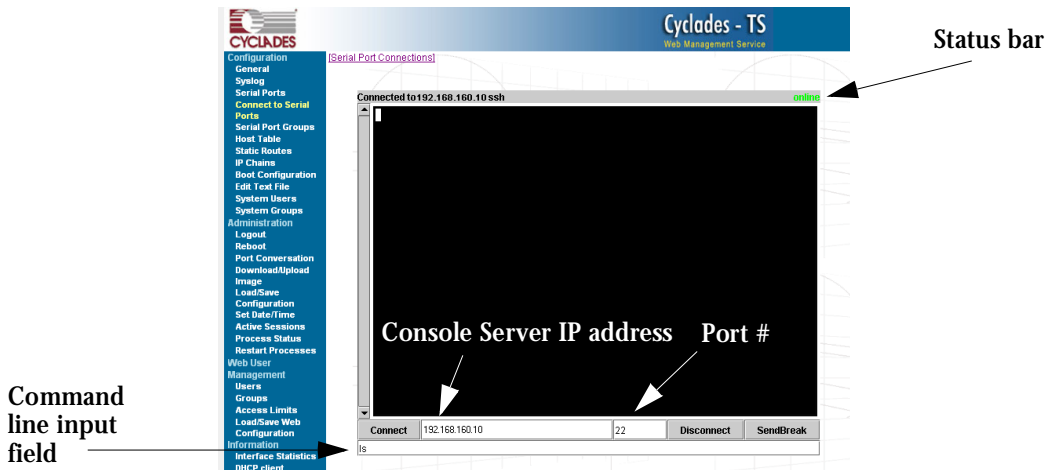


Figure 55: Port Connection page

Step 5: Log in.

If the port selected were configured for a ssh connection, a Login window will pop up. Login in this format: <username>:<socket_port number>. Then enter in the username's password.

Appendix H - Connect to Serial Ports from Web

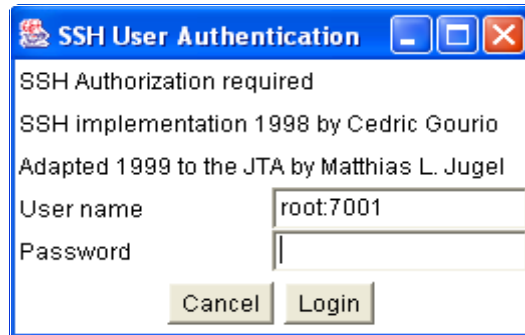


Figure 56: SSH User Authentication page

If the port selected were configured as `socket_server` or `raw_data`, and depending on how it is configured to be authenticated, log in by typing into the terminal or use the command line input field to send input into the terminal.

Step 6: Enter command.

Enter commands directly in the terminal or into the command line input field and hit Enter.

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.

Step 9: To reconnect to port.

Either refresh the current page or enter in the Cyclades-TS IP address and the port into the IP and port field. Then hit the Connect button. (For ssh connection, the port number should be 22.)

To connect to another serial port and/or Cyclades-TS, first make sure that you have disconnected from your current session. Then enter in the IP and port number into the appropriate fields and hit Connect. If you refresh the page now, the new connection will be lost and you will be returned to the original connection.

List of Wiz Application Parameters

Basic Parameters (wiz)

- Hostname
- System IP
- Domain Name
- DNS Server
- Gateway IP
- Network Mask

Authentication Parameters (wiz --auth)

- Authtype
- Authhost1
- Accthost1
- Authhost2
- Accthost2
- Radtimeout
- Radretries
- Secret

List of Wiz Application Parameters

Terminal Appearance Parameters (`wiz --tl`)

- Issue
- Prompt

Alarm Parameter (`wiz --al`)

- Alarm

Data Buffering Parameters (`wiz --db`)

- Data_buffering
- Conf.nfs_data_buffering
- Syslog_buffering
- Dont_show_DBmenu
- DB_timestamp
- DB_mode

List of Wiz Application Parameters

Sniffing Parameters (wiz --snf)

- Admin_users
- Sniff_mode
- Escape_char
- Multiple_sessions

Syslog Parameters (wiz --sl)

- Conf.facility
- Conf.DB_facility

Terminal Server Profile Other Parameters (wiz --tso)

- Host
- Term
- Conf.locallogins

List of Wiz Application Parameters

Access Method Parameters (wiz --ac <type>)

(CAS profile)

- Ipno
- Socket_port
- Protocol
- Modbus_smode
- Users
- Poll_interval
- Tx_interval
- Idletimeout
- Conf.group
- <sN>.serverfarm

(TS profile)

- Protocol
- Socket_port
- Userauto

List of 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

List of Figures

1. Console Access Server diagram	18
2. CAS diagram with various authentication methods	19
3. The Cyclades-TS3000 and cables	20
4. The Cyclades-TS2000 and cables	21
5. The Cyclades-TS1000 and cables	22
6. The Cyclades-TS800 and cables	23
7. The Cyclades-TS400 and cables	24
8. The Cyclades-TS100 and cables	25
9. The initial wizard configuration screen - console configuration method	37
10. Login page of Web Configuration Manager	40
11. Configuration & Administration Menu page	40
12. General page	41
13. The initial wizard configuration screen - telnet configuration method	47
14. Choose a free COM port	52
15. Port Settings	53
16. The /etc/hostname file with hostname typed in	54
17. Contents of the /etc/hosts file	55
18. Configuration and Administration page	73
19. Port Selection page	74
20. Serial Port Configuration page	74
21. Profile Section of Serial Port Configuration page	75
22. Serial Ports - Users Group Table Entry page	76
23. An example using the Clustering feature	104
24. Example of Centralized Management	109

List of Figures

25. Edit Text File page	114
26. Data Buffering section of the Serial Port Configuration page	119
27. Data Buffering section of the General page	120
28. DHCP client section	128
29. Page 1 of IP Chain filtering	130
30. Modbus application	149
31. Ports configured for Dial-in Access.	154
32. Terminal Server diagram	156
33. Sniff Session section of the Serial Port Configuration page	179
34. Syslog page 1.	188
35. Cable 1 - Cyclades RJ-45 to DB-25 Male, straight-through	232
36. Cable 2 - Cyclades RJ-45 to DB-25 Female/Male, crossover	233
37. Cable 3 - Cyclades RJ-45 to DB-9 Female, crossover	233
38. Cable 4 - Cyclades RJ-45 to Cyclades RJ-45, straight-through	234
39. Loop-Back Connector	234
40. Cyclades\Sun Netra Adapter	235
41. RJ-45 Female to DB-25 Male Adapter	236
42. RJ-45 Female to DB-25 Female Adapter	236
43. RJ-45 Female to DB-9 Male Adapter	237
44. RJ-45 Female to DB-9 Female Adapter	237
45. DB-25 Male to DB-9 Female Adapter	238
46. Pin assignment control	239
47. Cable 1 for TS100 - DB-9 Female to DB-9 Female, Crossover half duplex	240
48. Cable 2 for TS100 - DB-9 Female to DB-9 Female, Crossover full duplex	240

List of Figures

49. Cable 2 for TS100 - Block Connector to Block Connector, Crossover half duplex	.241
50. Cable 4 for TS100 - Block Connector to Block Connector, Crossover full duplex	.241
51. Data flow diagram of Linux-PAM	.263
52. Initial test	.288
53. Second screen, showing changed positions	.289
54. Serial Port Connection page	.301
55. Port Connection page	.301
56. SSH User Authentication page	.302

List of Tables

1. Hardware vs. Configuration Methods	32
2. Configuration Section	43
3. Web User Management Section	44
4. Administration Section	44
5. Information Section	45
6. Master Cyclades Configuration (where it differs from the CAS standard)	105
7. Cyclades-TS configuration for Slave 1 (where it differs from the CAS standard)	107
8. Cyclades-TS configuration for Slave 2 (where it differs from the CAS standard)	107
9. General Options for the Help Wizard	145
10. Help CLI Options - Synopsis 1	146
11. Help CLI Options - Synopsis 2	147
12. Modbus pslave.conf port-specific parameters (only where they differ from the standard CAS profile)	150
13. vi modes	216
14. vi navigation commands	216
15. vi file modification commands	216
16. vi line mode commands	217
17. Process table	222
18. Cyclades-TS power requirements	226
19. Cyclades-TS environmental conditions	226
20. Cyclades-TS physical specifications	227
21. Cyclades-TS safety specifications	227
22. Cables and their pin specifications	230

List of Tables

23. Which cable to use	231
24. TS100 Connector pin assignment.....	239
25. Parameters Common to CAS, TS, & Dial-in Access.....	243
26. Mostly CAS-specific Parameters	247
27. TS Parameters	258
28. Dial-in configuration Parameters.....	259
29. Files to be included in /etc/config_file and the program to use	285
30. CPU LED Code Interpretation.....	293
31. Required information for the OpenSSL package.....	295
32. Windows XP + JREv1.4.0_01 or 02	298
33. Redhat 7.3 + JREv1.4.0_01 or 02	298

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.

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.”

Glossary

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.

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.

Glossary

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-compliant 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)

Glossary

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 71
Alarm 138
Authentication 95

B

Basic Wizard 64
Battery 29
Block Connector 241

C

Cable Length 229
CAS Setup Scenario 256
CLI 32
Clustering 104
Command Line Interface 32, 63
Configuration using a Web browser 39
Connectors 229
CronD 112
Custom Wizard 35
Customization Process 281

D

Data Buffers 114
Default Configuration Parameters 32
DHCP 125
DNS Server 34
Domain 34

E

Ethernet 33

F

Filters 129
Flash Memory Loss 284

G

Gateway 33
 default 34
Generating Alarms 131

H

Hardware Specifications 226
Hardware Test 287
HyperTerminal 33

I

init process 280
IP Address 34

K

Kermit 33

L

Linux File Structure 213
Linux-PAM 262
loop-back connector 20

M

Minicom 33

Index

N

Netmask 34
NTP 152

P

Passwords 213
Port Test 287
pslave.conf file 243

R

Radius authentication 154
RJ-45 20
Routing Table 217
RS-232 Standard 228
RS-485 Standard 238

S

Secure Shell Session 218
Sendmail 138

Sendsms 138
serial ports 20
Snmptrap 138
Sun Netra Crossover cable 20
Syslog-n 191
System Requirements 31

T

Telnet 43
Terminal Appearance 206
Time Zone 211
TS100 Connectors 238

U

Upgrades 282
Using 69
Using the Wizard through your Browser 69

W

Wizard 34