BLACK BOX®
NETWORK SERVICES

MARCH 2004
Term Server 16 - 37687-R2
Term Server 8 - 37688-R2
Rack Term Server 16 - 40870-R2
Rack Term Server 8 - 40871-R2
102 Term Server- 41872-R2
104 Term Server - 41874-R2

Terminal Server User Guide

CUSTOMER SUPPORT INFORMATION

Order **toll-free** in the U.S 24 hours, 7 A.M. Monday to midnight Friday: **877-877-BBOX**
FREE technical support, 24 hours a day, 7 days a week: Call **724-746-5500** or fax **724-746-0746**
Mail order: **Black Box Corporation**, 1000 Park Drive, Lawrence, PA 15055-1018
Web site: **www.blackbox.com** * E-mail **info@blackbox.com**

Normas Oficiales Mexicanas (NOM) Electrical Safety Statement
INSTRUCCIONES DE SEGURIDAD

1. Todas las instrucciones de seguridad y operación deberán ser leídas antes de que el aparato eléctrico sea operado.
2. Las instrucciones de seguridad y operación deberán ser guardadas para referencia futura.
3. Todas las advertencias en el aparato eléctrico y en sus instrucciones de operación deben ser respetadas.
4. Todas las instrucciones de operación y uso deben ser seguidas.
5. El aparato eléctrico no deberá ser usado cerca del agua-por ejemplo, cerca de la tina de baño, lavabo, sótano mojado o cerca de una alberca, etc.
6. El aparato eléctrico debe ser usado únicamente con carritos o pedestales que sean recomendados por el fabricante.
7. El aparato eléctrico debe ser montado a la pared o al techo sólo como sea recomendado por el fabricante.
8. Servicio-El usuario no debe intentar dar servicio al equipo eléctrico más allá a lo descrito en las instrucciones de operación. Todo otro servicio deberá ser referido a personal de servicio calificado.
9. El aparato eléctrico debe ser situado de tal manera que su posición no interfiera su uso. La colocación del aparato eléctrico sobre una cama, sofá, alfombra o superficie similar puede bloquea la ventilación, no se debe colocar en libreros o gabinetes que impidan el flujo de aire por los orificios de ventilación.
10. El equipo eléctrico deber ser situado fuera del alcance de fuentes de calor como radiadores, registros de calor, estufas u otros aparatos (incluyendo amplificadores) que producen calor.
11. El aparato eléctrico deberá ser connectado a una fuente de poder sólo del tipo descrito en el instructivo de operación, o como se indique en el aparato.
12. Precaución debe ser tomada de tal manera que la tierra fisica y la polarización del equipo no sea eliminada.
13. Los cables de la fuente de poder deben ser guiados de tal manera que no sean pisados ni pellizcados por objetos colocados sobre o contra ellos, poniendo particular atención a los contactos y receptáculos donde salen del aparato.
14. El equipo eléctrico debe ser limpiado únicamente de acuerdo a las recomendaciones del fabricante.

15. En caso de existir, una antena externa deberá ser localizada lejos de las lineas de energia.
16. El cable de corriente deberá ser desconectado del cuando el equipo no sea usado por un largo periodo de tiempo.
17. Cuidado debe ser tomado de tal manera que objectos liquidos no sean derramados sobre la cubierta u orificios de ventilación.
18. Servicio por personal calificado deberá ser provisto cuando:
    a. El cable de poder o el contacto ha sido dañado; u
    b. Objectos han caído o líquido ha sido derramado dentro del aparato; o
    c. El aparato ha sido expuesto a la lluvia; o
    d. El aparato parece no operar normalmente o muestra un cambio en su desempeño; o
    e. El aparato ha sido tirado o su cubierta ha sido dañada.

FEDERAL COMMUNICATIONS COMMISSION
AND
CANADIAN DEPARTMENT OF COMMUNICATIONS
RADIO FREQUENCY INTERFERENCE STATEMENTS

This equipment generates, uses, and can radiate radio frequency energy and if not installed and used properly, that is, in strict accordance with the manufacturer's instructions, may cause interference to radio communication. It has been tested and found to comply with the limits for a Class A computing device in accordance with the specifications in Subpart J of Part 15 of FCC rules, which are designed to provide reasonable protection against such interference when the equipment is operated in a commercial environment. Operation of this equipment in a residential area is likely to cause interference, in which case the user at his own expense will be required to take whatever measures may be necessary to correct the interference.

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

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

Le présent appareil numérique 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 publié par le ministère des Communications du Canada.

CE **Caution:** the Console Server is approved for commercial use only.

About this manual

Purpose of this manual

This manual tells you how to install, configure and use the Black Box Terminal Server communications servers.

Who this manual is for

This manual is aimed at users who want to connect serial devices directly to LANs and WANs. This manual requires a working knowledge of using personal computers and associated operating systems, as well as experience in installing host cards and peripherals.

Fast Contents

About this manual 5
Fast Contents 6
Contents 7
Chapter 1 Introduction 23
Chapter 2 Installation 32
Chapter 3 Terminals on mutli-user systems 50
Chapter 4 Setting up dial-in modem ports 58
Chapter 5 Modem authentication and logging 66
Chapter 6 Dialout modem ports setup 75
Chapter 7 Vmodem (Virtual modem) 85
Chapter 8 Printing 94
Chapter 9 Other devices setup 110
Chapter 10 The menu interface 121
Appendix A Command Line Interface 156
Appendix B 48V DC Rack Terminal Server 169
Appendix C Troubleshooting 174
Appendix D Cabling 193
Index 207

Contents

ABOUT THIS MANUAL 5

Purpose of this manual 5

Who this manual is for 5

FAST CONTENTS 6

CONTENTS 7

CHAPTER 1 INTRODUCTION 23

About the Terminal Server 24
Terminal Server Features 26
Hardware 26
Software 27
Security 28
Hardware Overview 29
Hardware description for Terminal Server 29
Hardware description for Rack Terminal Server 30
Hardware description for 102/104 Terminal Server 31

CHAPTER 2 INSTALLATION 32

Connecting to your Network 33
- 10BASE-T (twisted pair) 33
- 10BASE2 (Thin Ethernet) 33
- AUI port 33
- 10/100BASE-T 33

Switching on Terminal Server 34

Communicating via ARP 35

Communicating via a Terminal or PC 36

The Menu System 37
- Connections Menu 39
- Administration Menu 40
- Server Configuration Menu 42
- Port Setup Menu and Beyond 44

Tips 46
- Copy Command 46
- Connecting via BOOTP (for Unix systems only) 46
- Saving and downloading configurations 48
- Domain Name Server (DNS) 49
- Reassigning your Terminal Server to a New Network 49
- Updating Terminal Server Firmware 49

CHAPTER 3 TERMINALS ON MUTLI-USER SYSTEMS 50

Introduction 51
Terminal Port Configuration 52
Host Table Setup 54
Making a Connection 55
Tips 57
Connecting via 'fixed ttys' 57
Multisessions on terminals/PCs 57
Gateway Tables 57

CHAPTER 4 SETTING UP DIAL-IN MODEM PORTS 58

Introduction 59
Dial-in Port 60
The host 62
The modem 63
Client login 64
Tips 65
Domain Name Server (DNS) 65
WINS Server 65
MOTD 65
Gateway notes 65

CHAPTER 5 MODEM AUTHENTICATION AND LOGGING 66

Introduction 67
User authentication/logging 68
The host 71
Basic authentication 71
User services authentication 71
Logging 73
Tips 74

CHAPTER 6 DIALOUT MODEM PORTS SETUP 75

Introduction 76
Configuration 77
The host 78
For dial-out connections on Unix 78
For dial-out connections on Windows ® systems 78
Routing 79
Remote Access Systems 80
Dial-out PAP Authentication 82
Remote site devices 83
Tips 84

CHAPTER 7 VMODEM (VIRTUAL MODEM) *85*

About Vmodem (Virtual modem) ***86***
Configuring ports to use Vmodem ***87***
Configuring ports to use Vmodem in Normal Mode *87*
Making a Call using Vmodem in Normal Mode *89*
Disconnecting a Call in Vmodem Normal Mode *89*
Configuring Vmodem to use Dial on DTR mode *90*
Making a Call using Vmodem in Dial on DTR Mode *91*
Disconnecting a Call in Vmodem Dial on DTR Mode *91*
Setting/Modifying up Vmodem responses ***92***
Vmodem AT Commands ***93***

CHAPTER 8 PRINTING 94

Introduction **95**
Using ioland **96**
Configuration *97*
The Host *98*
Using LPD **99**
Configuration *99*
Accessing the Printer *101*
LPD printing from DOS/Windows ® *102*
LPD Printing from BSD Unix and Linux *103*
LPD Printing from SYS V Unix *104*
LPD printing from AIX *104*
LPD printing from HP/UX *104*
Using RCP **105**
Configuration *105*
The Host *106*
Using RCP with Unix System V line printer spoolers. *107*
RCP printing on a spooler system based on BSD Unix *108*
Setting up RCP printing on AIX *109*

CHAPTER 9 OTHER DEVICES SETUP 110

Introduction 111
Reverse Telnet Port Configuration 112
The Host 113
Black Box IOLAND Utility 114
Mandatory arguments 115
Optional arguments 116
Example daemon configuration file 119
Tips 120

CHAPTER 10 THE MENU INTERFACE 121

Introduction to menu commands 122
Toggle fields 122
Fast keys 123
Connections menu 124
Port setup menu 126
Hardware 127
User 128
Flow control 129
IP address 130
Options 131
Keys 132
Access 133
Administration menu 135
Extra statistics screens 136
Access menu 137
Remote access sites 138
Remote site devices 140
Authentication/Logging 142
Change password options 144
Gateway menu 145
Host Address menu 146
Kill command 146
Lines menu 147
Access 148
Flow control 148
Hardware 148
Network connections 149
Options 149
Terminal 150
Port menu 150
Quit command 150
Reboot command 150
Server configuration menu 151
Statistics screens 154
Trap function 155

APPENDIX A COMMAND LINE INTERFACE 156

Introduction 157
Using the CLI 158
System administration 159
Basic configuration 160
Command descriptions 161

arp 161
clear 161
connect 161
copy 162
dial 162
disconnect 162
exit 162
facreset 162
gateway 162
help 163
host 163
kill 163
lock 163
logout 163
prov 163
reboot 164
resume 164
rlogin 164
save 164
set 165
set admin 165
set menu 165
set modem 165
set term 165
set port 166

set port [number] 166
set port [number] [access, flow, hardware, options, tcp, user] 166
set server 166
set slip [IP address] 166
set ppp [IP address] 166
set password [admin] or [login] 166

show 167

show ports *167*
show lines *167*
show statistics *167*
su *167*
telnet *167*
test *168*

APPENDIX B 48V DC RACK TERMINAL SERVER *169*

Introduction *170*
Installing the Rack Terminal Server 48V DC *171*
Installation *171*
Electrical Supply Details *171*
Safety Earth *172*
Fusing *172*
Electrical Safety Guidelines *173*
Connecting up your Rack Terminal Server *173*
Disconnecting your Rack Terminal Server *173*

APPENDIX C TROUBLESHOOTING *174*

Introduction ***175***
Terminals/PC Problems ***176***
Printer Problems ***178***
Modem problems ***180***
Unit still does not communicate ***181***
Resetting Your unit ***182***
Using the Statistics screens ***183***
ETH/TTY/GATEWAY *183*
IP/ICMP/UDP *184*
TCP *184*
Users *184*
Framed Link Status *185*
Netstat *186*
Gateway *186*
SLIP *186*
Clear counters *186*
Restore counters *187*
Port Status *187*
Line status *187*
LPD Status *188*
PPP Status *188*
Using SNMP ***188***
Diagnostics ***189***
Entering the Diagnostic Menu *189*
Self-test *189*
Monitor *189*
Download *190*
Ethernet Interface *190*
Reset *191*
Reset all settings *191*
Reset password *191*
Reset IP address *191*
Reset product name *191*
Reset Ethernet address *191*
Quit *191*

APPENDIX D CABLING 193

Introduction 194

Serial port connectors on the Terminal Server unit 195

Serial port connector guide 195

RS232 DB25 female DTE 195

RS232 RJ45 DTE socket 197

RS422 RJ45 DTE socket 198

Standard modem cables 199

Terminal Server DB25 DTE to Modem DB25 DCE 199

Cable diagram 199

Connector pinout table 199

Rack Terminal Server and 102/104 Terminal Server RS232 RJ45 DTE to Modem DB25 DCE 200

Cable diagram 200

Connector pinout table 200

Standard Terminal/PC cables 201

Terminal Server DB25 DTE to Terminal DB25 DTE 201

Cable diagram 201

Connector pinout table 201

Terminal Server DB25 DTE to PC DB9 DTE 202

Cable diagram 202

Connector pinout table 202

Rack Terminal Server and 102/104 Terminal Server RJ45 DTE to Terminal DB25 DTE 203

Cable diagram 203

Connector pinout table 203

Rack Terminal Server and 102/104 Terminal Server RJ45 DTE to PC DB9 DTE 204

Cable diagram 204

Connector pinout table 204

Printer cables with hardware flow control 205

Terminal Server DB25 DTE to Printer DB25 DTE 205

Cable diagram 205

Connector pinout table 205

Rack Terminal Server and 102/104 Terminal Server RJ45 male to printer DB25 DTE 206

Cable diagram 206

Connector pinout table 206

INDEX 207

Chapter 1 Introduction

You need to read this chapter if you want to...

You need to read this chapter if you want an overview of the Terminal Server product.

This chapter provides introductory information about the Black Box Terminal Server, its associated components, software and configuration utilities.

This chapter includes the following sections;

- **About the Terminal Server** on page **24**
- **Terminal Server Features** on page **26**
- **Hardware Overview** on page **29**
- **Hardware description for Terminal Server** on page **29**
- **Hardware description for Rack Terminal Server** on page **30**
- **Hardware description for 102/104 Terminal Server** on page **31**

About the Terminal Server

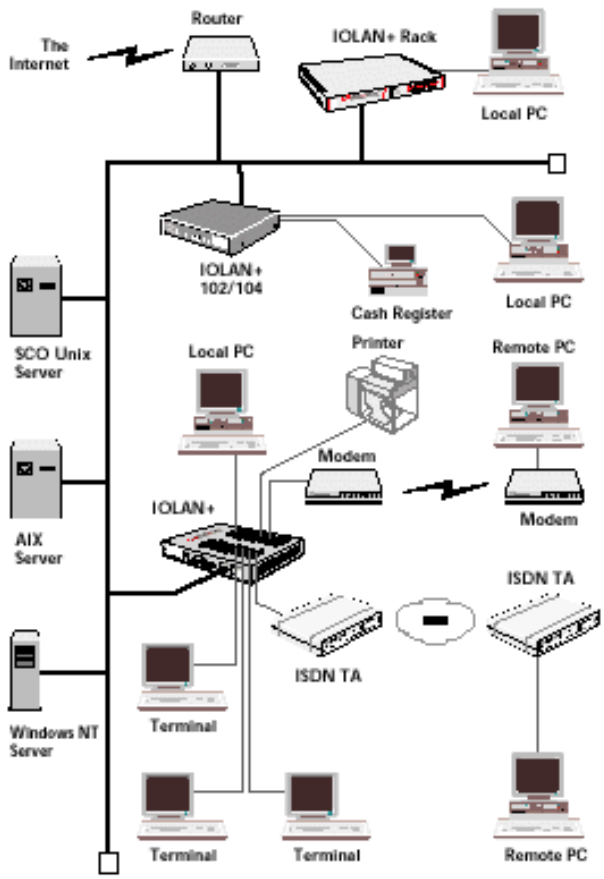
The Terminal Server is a unique Ethernet TCP/IP communications / terminal server allowing serial devices to be connected directly to LANs and WANs. The 2, 4, 8 or 16 serial ports enable Terminal Server to connect to a wide range of devices including:

- Modems for remote access and Internet access
- ISDN adapters for branch remote access and Internet access
- Terminals for multi-user Unix systems
- PCs using terminal emulation or SLIP/PPP
- All types of serial printers
- Data acquisition equipment (manufacturing, laboratory, etc.)
- Retail point-of-sale equipment (bar coding, registers, etc.)

The performance and flexibility of Terminal Server allows you to use a wide range of high speed devices in complex application environments. These operating systems include:

- Windows ® 95/98
- Windows NT ®
- Citrix Winframe
- SCO Unix & Gemini
- IBM AIX
- Sunsoft Solaris
- Hewlett Packard HP-UX
- Data General DG/UX
- All other variants of Unix (BSD, Linux, IRIX, etc.)

This configuration diagram shows many of the features available on the Terminal Server communications server:



Terminal Server Features

Terminal Server is a TCP/IP communications server with 2, 4, 8 or 16, RS-232 or RS-422 ports for making serial network connections. It attaches to your TCP/IP network and allows serial devices such as modems, terminals and printers to access the network.

Hardware

The Terminal Server hardware features include:

- 2, 4, 8 or 16 serial lines, fully configurable with port speeds up to 115.2 kbps.
- RJ45 connectors on Terminal Server and 102/104 Terminal Server or DB25 connectors on Terminal Server.
- Full modem control using DTR, DSR, CTS, RTS and DCD.
- FLASH memory for downloading firmware releases.
- 102/104 Terminal Server has 10BASE-T or 10/100BASE-T interfaces.
- Terminal Server and Rack Terminal Server have either autosensing 10BASE-T / 10BASE2 / AUI or 10/100BASE-T interfaces.
- Auto sensing power supply; 110-250V AC (48-60V DC option available on Terminal Server).
- LEDs for diagnostic testing.
- Self-test on power-up.
- Rack mount or tabletop design.

Software

The Terminal Server software features include:

- Support for TCP/IP and UDP protocols including telnet and rlogin.
- Remote access support including PPP, SLIP and CSLIP.
- Printer support via lpd, rcp, and utilities.
- Modem support via PPP and utilities.
- Utilities provide ‘fixed tty’ support for Unix systems.
- A window oriented menu interface with pop-up menus and on screen help (command line also available).
- ARP or BOOTP for network based setup.
- Dynamic statistics displays and line status reporting for fast problem diagnosis.
- Multi screens on terminals.
- Full support of SNMP MIBs, allowing remote configuration via SNMP as well as statistics gathering.
- Interoperability with IP routing through gateway tables.
- Domain Name Server support.
- WINS support for Windows ® environments.
- Port configuration copy and save functions.

Security

The Terminal Server security features include:

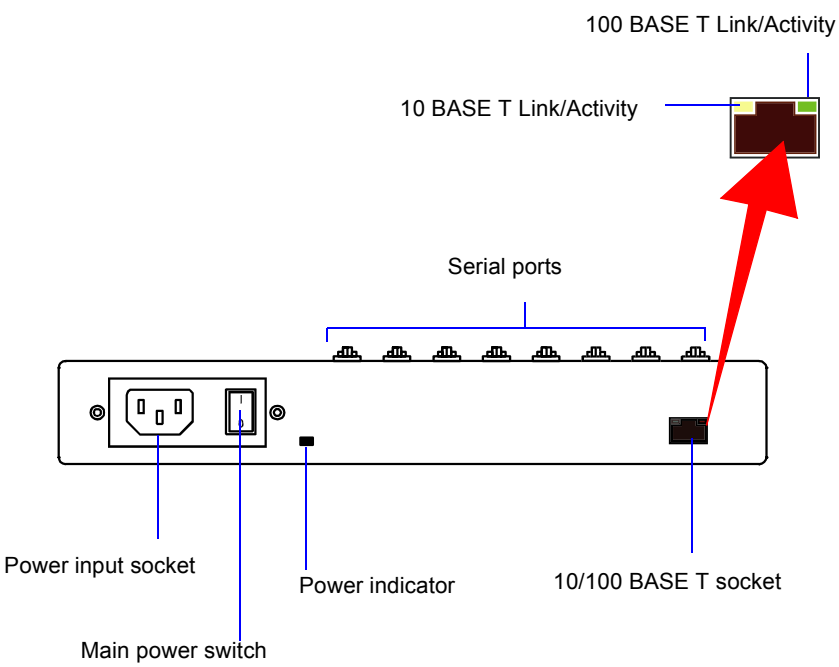
- Supervisory and port password.
- Port locking.
- Authentication with PAP support.
- Per user access level assignment.
- Service logging.
- Logging facility for audit and billing.
- Modem auto reset.

Hardware Overview

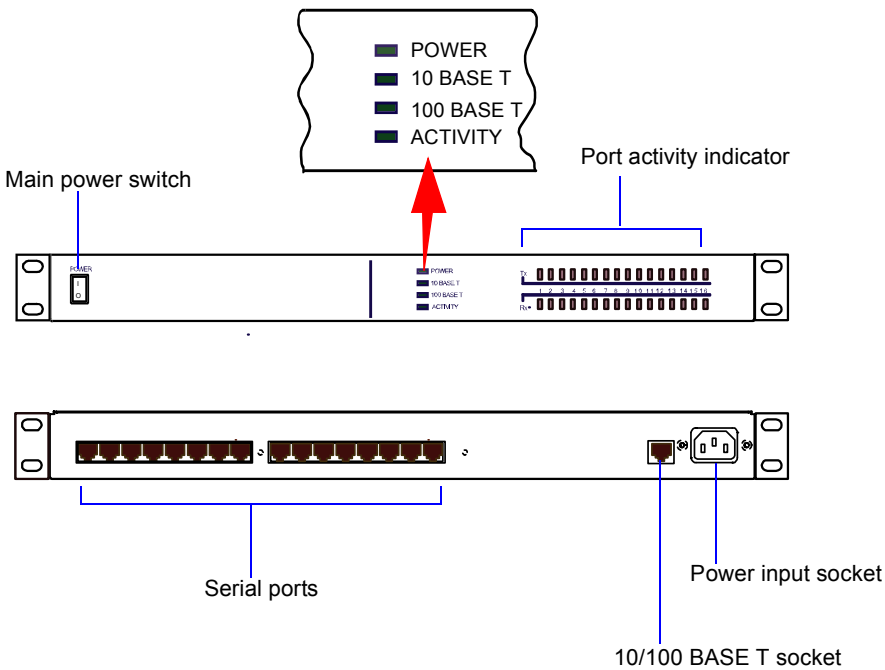
The following table and diagrams describe the units:

Model	Type	No. Ports	Connector	Interface
102/104 Terminal Server	Table Top	2,4	RJ45	RS-232
Terminal Server	Table Top	8,16	DB25	RS232
Rack Terminal Server	Rack Mount	4, 8, 16	RJ45	RS-232

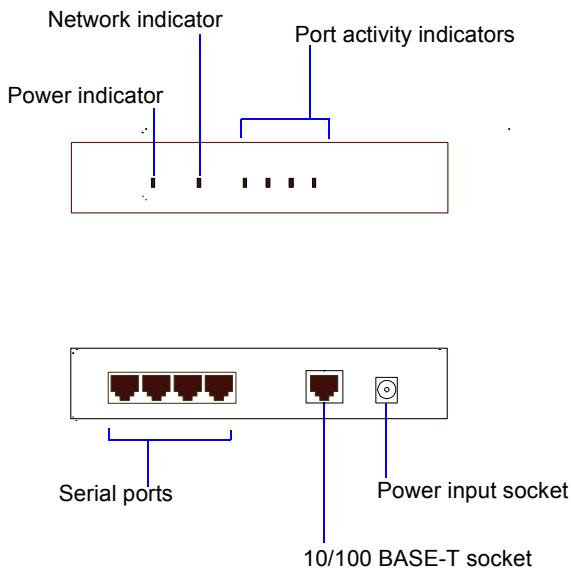
Hardware description for Terminal Server



Hardware description for Rack Terminal Server



Hardware description for 102/104 Terminal Server



Chapter 2 Installation

You need to read this chapter if you want to...

You need to read this chapter if you want information about installing your Terminal Server product.

This chapter provides information about installing the Black Box Terminal Server including connecting to your network, configuring communications as well as information on the menu system and general tips.

This chapter includes the following sections;

- **Connecting to your Network** on page **33**
- **Switching on Terminal Server** on page **34**
- **Communicating via ARP** on page **35**
- **Communicating via a Terminal or PC** on page **36**
- **The Menu System** on page **37**
- **Tips** on page **46**.

Connecting to your Network

First connect Terminal Server to a network then begin configuring the unit for your application. Additional information on configuring modems and printers follows.

Terminal Server and Rack Terminal Server connect to your ethernet network via one of the following (depending on your hardware model):

- Auto-sensing 10BASE-T (twisted pair)
- Auto-sensing 10BASE2 (thin)
- Auto-sensing AUI
- 10/100BASET

102/104 Terminal Server connect using either:

- 10BASE-T (twisted pair)
- 10/100BASE-T

10BASE-T (twisted pair)

Attach the RJ connector from a hub directly to Terminal Server twisted pair port.

10BASE2 (Thin Ethernet)

Attach a BNC T connector directly to your Terminal Server. If your unit is the termination point for the cable you need to add a terminator. Always ensure that each segment of the thin Ethernet cable is at least 0.5m in length. The maximum length for a thin Ethernet cable is 185 metres.

AUI port

The AUI connector allows an external transceiver to be connected. This allows a number of different interfaces to connect including 10BASE5 (or thick) and fibre optic transceivers.

Attach the RJ45 connector from a hub directly to the Terminal Server port.

10/100BASE-T

Attach the RJ connector from a hub directly to the Terminal Server 10/100BASE-T port.

Switching on Terminal Server

The Terminal Server power supply accepts input voltages in the range 110 to 240V AC, allowing it to be used world-wide. The 102/104 Terminal Server has an external power supply unit.

After you connect your LAN interface, you can power up the unit. The green power indicator at the side (or front for rack and 102/104 units) should be lit. If the unit fails to power up with the green power indicator lit, disconnect the unit and contact your dealer for help.

The Terminal Server firmware may be compressed, and this takes a short time to decompress before running.

During this phase the network LEDs will light alternately to indicate that decompression is in progress.

The green Ethernet indicators show the active connections. It remains lit and blinks when LAN traffic is active.

> Note:
> To change your Ethernet media, you will need to reboot the unit to activate the connector.

If your unit has 10BASE-T, 10BASE2 and AUI connectors, then the green ethernet indicators show the active connection. The indicators remain lit and blink when LAN traffic is active.

If you have an Rack Terminal Server unit with 10/100BASE-T, then the Ethernet indicators will light green to indicate either 10Mbit or 100Mbit link, and the Activity light flickers to indicate LAN traffic.

If you have a Terminal Server or 102/104 Terminal Server with 10/100BASE-T, then the Ethernet will light green to indicate a 100Mbit link, and orange to indicate a 10Mbit link. The LED will flicker to show LAN traffic.

You are now ready to begin communicating with your Terminal Server. You can connect to the unit in different ways: via a terminal or PC on port 1, or using ARP or BOOTP. Using ARP is the preferred method for both Windows ® and Unix, however a terminal or PC attached to port 1 is often used.

BOOTP setup is for Unix users only. Choose the appropriate method for your application. Third party BOOTP packages are available for Windows ®

Communicating via ARP

Your Terminal Server supports the 'Address Resolution Protocol' (ARP). It allows you to temporarily connect to your Terminal Server to assign a permanent IP address. If you prefer to use a terminal or PC attached to Terminal Server see **Communicating via a Terminal or PC** on page **36**.

To do this proceed as follows;

1. From a local Unix host, type the following:

   arp -s a.b.c.d aa:bb:cc:dd:ee:ff

   (where a.b.c.d is the IP address you want for Terminal Server, and aa:bb:cc:dd:ee:ff is the Ethernet address of your Terminal Server, found on the bottom of the unit itself).

2. On a Windows ® NT/98 system, the arp command is slightly different (using dashes instead of colons):

   arp -s a.b.c.d aa-bb-cc-dd-ee-ff

3. Whether you use Unix or Windows ® to run arp, you are now ready to telnet to Terminal Server. Here is the sequence to use:

   arp -s 192.168.209.8 00:80:d4:00:33:4e
   telnet 192.168.209.8
   password>
   local>

4. At the password prompt, press the **Enter** key since this is not set yet. The IP address still needs to be configured on the unit (ARP has only allowed you to connect to the unit so far).

> Note
>
> If there are any errors, recheck both the IP and Ethernet addresses you keyed in (this is the most common error here). See **Appendix B Troubleshooting** for more information on problems.

You can now skip the next section and go straight to **The Menu System** on page **37**

Communicating via a Terminal or PC

You can connect to Terminal Server using a terminal or PC (with a terminal emulation package such as Hyperterm).

1. Connect a terminal or your PC to port 1. The Terminal Server serial ports are DTE type RS-232 ports. When connecting a terminal/ PC directly (without modems), the RS-232 signals need to be crossed over (‘null modem’ cable). See **Appendix D Cabling** for pinout information.
2. For a terminal/PC to communicate with a server, set it to the following: 9.6 kbps, eight data bits, one stop bit, software flow control, no parity.

   After powering up your Terminal Server, you are prompted to enter a ‘Local login:>‘.

3. You can just hit any character and at this point (the character is required).

   The next prompt displayed is local>, which is the Command Line Interface (CLI) prompt.

> Note
>
> If there are any problems, check the cable you are using (this is the most common error). Port 1 is configured to provide error messages should any problems occur. See **Appendix B Troubleshooting** for more information on problems.

You can now move to The Menu System. See **The Menu System** on page **37**.

The Menu System

You should now be at the Command Line Interface (CLI) of the Terminal Server as designated by the local> prompt. If you would like to continue in CLI mode refer to **Appendix A Command Line Interface**, but we recommend the menu system.

1. Set the terminal emulation type and begin using the menus.

   The following are the terminal options:

   ansi, dumb, vt100, wyse50, wyse60, tvi925, ibm3151, vt320, falco50, hp700

2. The default setting is ‘dumb’. To set the menu interface to your emulation simply type set term with your option.

   Example:

   local> set term ansi

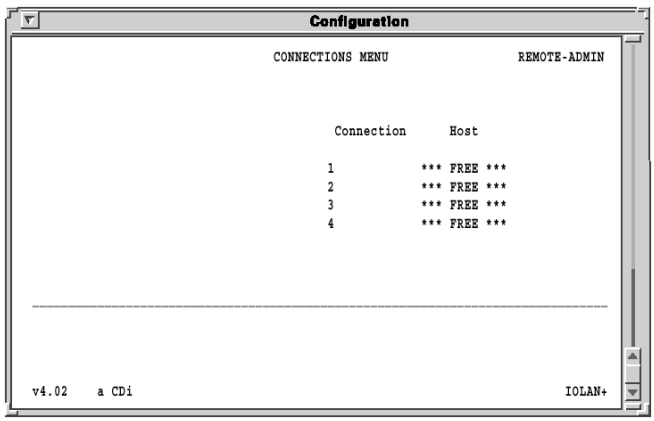
   > Note
   > For Falco50 type local> set term falco

3. To switch from the command line interface to the menu interface, at the local> prompt enter:

   set menu

The Connections Menu should now be displayed.

This menu displays the current state of the four possible connections. There are no active connections.



The firmware version of Terminal Server is located on the lower left hand portion. The wording ‘REMOTE-ADMIN’ in the upper right signifies you are remotely telneted into Terminal Server (and will read ‘Terminal: 1’ if you are using a terminal/PC into port 1.)

The keys used to move about in the menus depend on the terminal emulation you are using. The arrow keys should all work. The TAB key is very important for moving between fields.

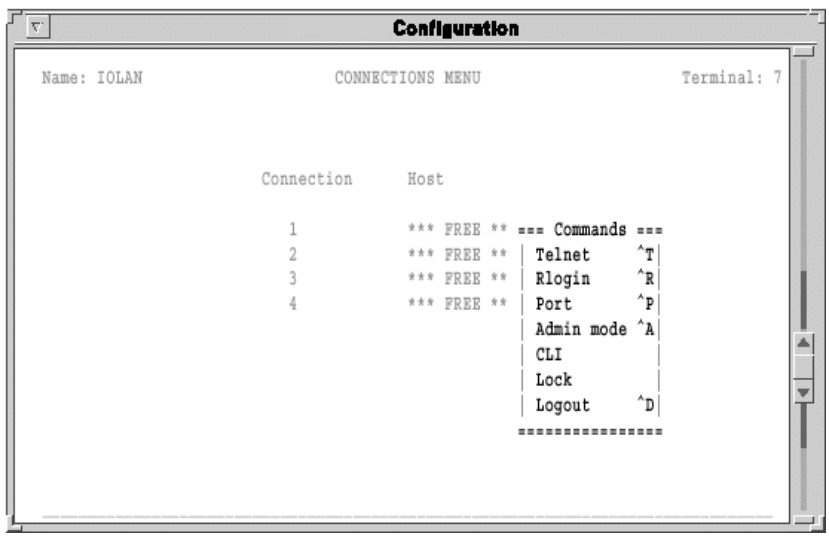
Backspace and DEL should work, but depend on the emulation.

ESC (the escape key) will move you back one menu.

> Note
>
> If there is a problem with your emulation, you can try a different emulation mode. See **Appendix B Troubleshooting**for more information.

An accelerator key can be used to jump to an option within a menu and is the first letter of the option.

Select connection '1' on the Connections Menu and press the **Enter** key. The Commands pop-up menu is displayed. There are a number of options available from this menu.



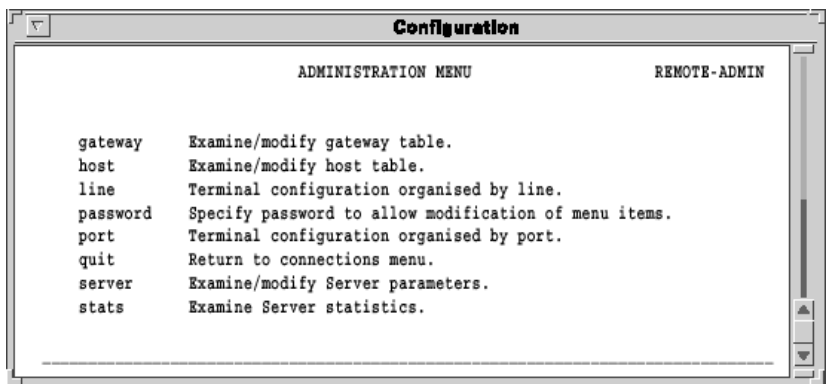
Before communication across the network can be established the Terminal Server must be assigned a network IP address. This is accessed through the Administration Menu.

Select the Admin mode field and press the Enter key.

> Note
>
> If you are telneted into Terminal Server, the telnet, rlogin and port options do not appear on the Commands pop-up menu.

Administration Menu

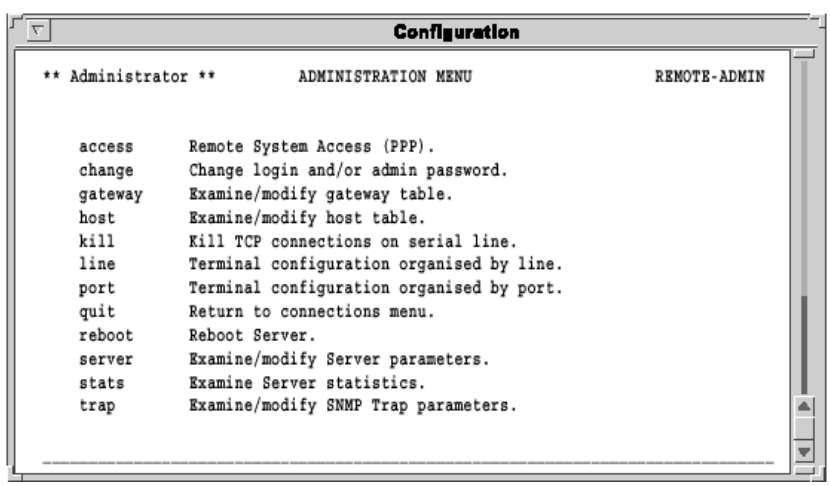
The top level Administration Menu appears as follows:



1. Select the Password field and press the **Enter** key. Use the factory default password here: this is iolan (no caps).

> Note:
>
> This password level will time-out in four minutes if there is no activity. This is for security reasons and will take you back to Administration Menu (view level).

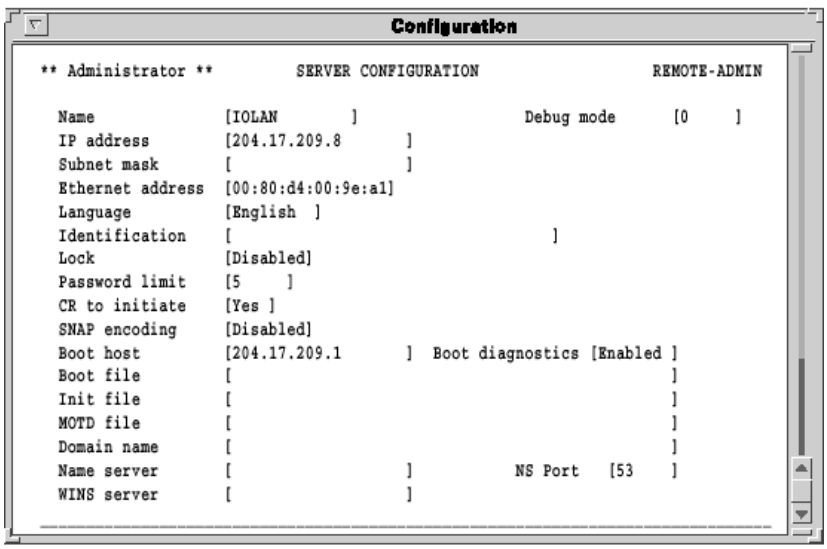
The Administration Menu is redisplayed, it now has some extra fields (access, change, kill, reboot, trap).



2. Select the server entry and press the **Enter** key. This takes you into the Server Configuration Menu.

There are a number of fields in the Server Configuration menu which are explained in **Chapter 10 The menu interface**. At this point proceed as follows;

1. Give the Terminal Server an IP address and a name.



2. The important fields that you need to fill in are as follows:

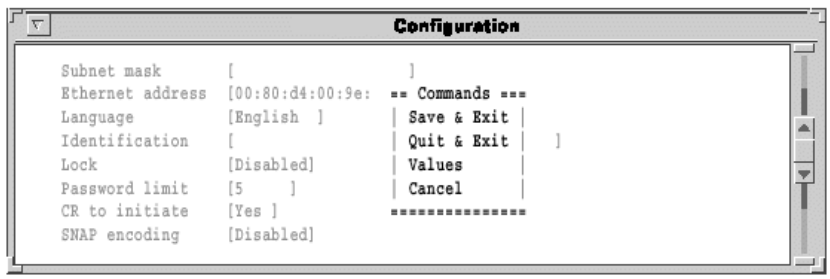
   Name: In the example above the communications server name has been set to IOLAN. It is a good idea for the Terminal Server name entered here to match the name entered in the host machine's domain name server.

   > Note
   >
   > For more information about domain name servers, consult your operating system manuals.

   IP Address: This address must be set to a value that is consistent with the network the Terminal Server is on.

3. Having filled in the fields press the **Enter** key. This brings the Commands pop-up menu as shown in the next picture.

   > Note
   >
   > The Ethernet address is factory set. This address is uniquely assigned to the Terminal Server and MUST NOT be changed.



4. Select the Save & Exit field and press the **Enter** key. Other options are Quit & Exit, which does not save the changes before exiting this menu, Values, which will display the optional values for this field if available, and Cancel, which will take you back to this screen for more editing.
5. You have now set up the unit with a new IP address. This should be confirmed with the message:

   IP CHANGED—PLEASE REBOOT

6. Reboot the communications server to activate the new IP address using the reboot command. The IP address and/or subnet mask are the only parameters that when changed necessitate rebooting.

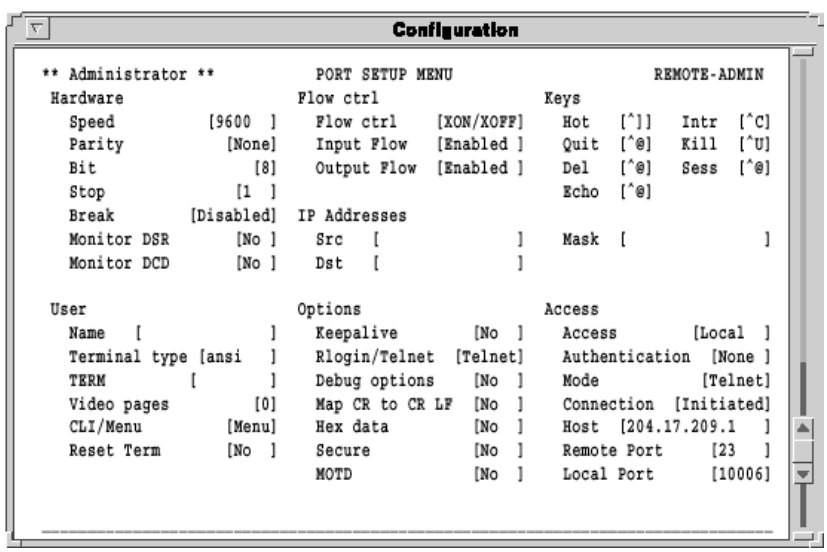
Your communications server is now ready to configure for terminals on multi-user systems or modems, printers and other devices. The next sections deal with each of these.

If you've got a good feel for the menu system, you should proceed to the section appropriate for your application.

If you'd like a full review of the menu system refer to section 9, The Menu Interface later in this guide. For more information about the Command Line mode, consult **Appendix A Command Line Interface**.

All of the procedures are based around the Port Setup Menu. This is accessed through the Administration Menu (password level). Remember, that if you are not in the password level, you can only view the information, not change it.

Here is the Port Setup Menu:



This menu allows the user to set up all the parameters associated with a port. The administrator can alter the set-up of any port on the communications server while a user can only alter the set-up for their own port.

This menu is divided into the following sections:

Menu option	Description
Hardware	Defines port type and is used for setting up the hardware configuration of the modem, terminal, printer or PC session. This section is always used.
User	Defines various user parameters such as name and terminal type. Most fields are used in this section.
Flow Control	Defines the various flow control options used by the Terminal Server. This section is always used.
IP Addresses	Deals with remote access via PPP/SLIP sessions.
Options	Deals mainly with the telnet options. This section is the least used.
Keys	Defines the various accelerator keys that the Terminal Server responds to and can be used for convenience.
Access	Controls the type of the connection made from this port. This is the most important section in defining a port.

If you're ready to install terminals, printers and modems, proceed to the appropriate section. For a good review, go to **Chapter 10 The menu interface**.

Tips

Copy Command

The Terminal Server has a copy command that allows you to copy the setup of one port to another. You will need to get to the CLI (from the Connection menu) and use the following syntax.

> Note:
> To get back to the menu system once in the CLI, type set menu at the command line.
>
> **local> su**
> **password>**
> **ADMIN:local> copy 1 2 3 4 5**
> **ADMIN:local> set menu**
>
> The commands above would copy the configuration of port number 1 to ports 2, 3, 4 and 5 (and return you to the menu system).

Connecting via BOOTP (for Unix systems only)

Your Terminal Server supports BOOTP which allows the communications server to dynamically configure itself on startup. Upon startup your Terminal Server sends four BOOTP broadcast requests if it has no IP address. This broadcast request packet contains the Ethernet address of your unit.

The request is received by all hosts on the network and is checked against a file to find a match. This data base file will normally be /etc/bootptab and will be of the following format:

 # bootptab description

iolan:ht=ethernet:ha=0080d400024e:

:hd=/tftp:

:bf=iolan.DL:

:ip=192.168.209.8:

Where:

ht is the type of network

ha is the Ethernet address on back of your unit

hd is the home directory for specifying Terminal Server firmware (optional)

bf is the name of Terminal Server firmware (optional)

ip is the IP address you want to use

> Note
> This BOOTP implementation is a subset and not a full implementation of the RFC.

> Note
> The most common error is bad information in the /etc/bootptab file (recheck it). See **Appendix B Troubleshooting** for more information.

You can now move back to The Menu System in this chapter.

Saving and downloading configurations

It is possible to save the configuration of your Terminal Server. This is convenient for loading multiple communications servers with the same setup. It is also advisable as a backup method.

If the boot file name has the extension ".cfg" (eg iolan.cfg), it will be loaded as a configuration file rather than a boot file.

This allows the administrator to configure one Terminal Server, save its configuration and automatically configure subsequent units via bootp.

Should the configuration of your Terminal Server ever be corrupted because of user error or damage, it is an advantage to have the configuration stored somewhere for easy re-installation.

This can be achieved by uploading the configuration of the unit to a host on the network. To do this, enter the Communications Server Menu from the Administration Menu. Select the Init file entry of this menu.

Set this to the full pathname of the file in which you wish to store the configuration. Set Boot host to the host machine you wish the file to reside within and save these entries.

Boot host: rockvegas (or ip address)
Init file: /tftp/term_serv.cfg

Log onto the host machine in the normal manner and create the file you have specified in the Terminal Server menu, this could be as shown in the next picture:

touch term_serv.cfg

Note

This file must exist with the correct read/write permissions before you can write to it. This can be accomplished by pressing the **Enter** key and selecting the CLI option in the pop up menu. At the iolan> prompt, use the CLI as the administrator by typing:

su
and enter the password and type:
save config
This uploads the communications server port configurations to the host in a format that can be downloaded at a later date.

Note

This does not save any of the settings configured in the Server Configuration Menu, including the IP address, language, name, subnet mask, etc.

Terminal Server will now automatically download this configuration on reboot. Remember that whenever you change a setting on the unit, it will be overwritten the next time the unit is rebooted unless the new configuration is saved.

Domain Name Server (DNS)

Terminal Server can be configured to take advantage of your network's Domain Name Server (DNS). This is done from the server in the Administration Menu by keying in the IP address of your DNS in the Name server field. Fill in the Domain name field as well.

Reassigning your Terminal Server to a New Network

If you need to attach your Terminal Server to a different network with a new IP address, it is possible to reset it to factory default condition using the following procedure:

1. Power on the unit.
2. Wait 30 seconds.

> Note
>
> If firmware is compressed, then network LED will alternately light for approximately an additional 30 seconds.

3. Hold down the RESET button for 15 seconds.
4. Release the button.

   After this is done, the unit will start sending BOOTP request packets.

This procedure is useful for factory defaulting units which cannot be reached via TCP/IP. This includes reassigning a programmed unit to a network to which the previously assigned IP address does not belong.

Updating Terminal Server Firmware

Firmware can be downloaded across the network using tftp protocol if the host machine and file name are set in the boot host and boot file entries of the server menu. These entries are checked at start up and if they have been configured, the relevant file will be downloaded.

> Note:
>
> tftp must be enabled on the relevant host as it is disabled by default

Chapter 3 Terminals on mutli-user systems

You need to read this chapter if you want to...

You need to read this chapter if you want information on setting up a terminal for use with your Terminal Server product.

This chapter provides information on how to setup a terminal, and other tips such as the concept of ‘fixed ttys’, multiscreens, the copy command, TERM features, etc.

This chapter includes the following sections;

- **Introduction** on page **51**
- **Terminal Port Configuration** on page **52**
- **Host Table Setup** on page **54**
- **Making a Connection** on page **55**
- **Tips** on page **57**

Introduction

Terminal Server is used extensively for connecting terminals, printers and modems on multi-user Unix systems, especially in retail applications. These Unix systems include SCO Unix, IBM AIX, HP-UX, Data General's DG/UX, etc. This chapter deals with terminals and/or PCs using emulation packages (such as Hyperterm).

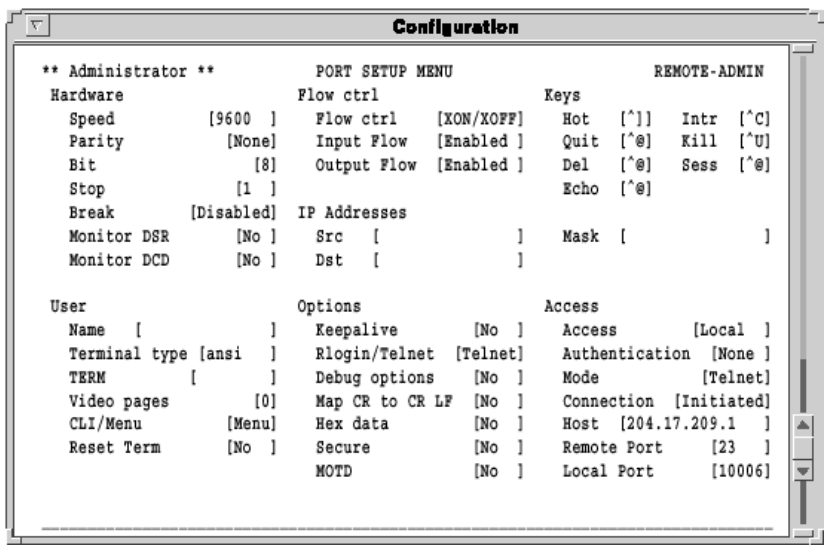
In many applications, the users need to be 'direct connected' to a specific Unix host so that they see the login prompt automatically. This is helpful in securing your system, or in environments where the users need to be in one application only.

This chapter will show how to setup a terminal, and other tips such as the concept of 'fixed ttys', multi screens, the copy command, TERM features, etc. Consult **Appendix D Cabling**, for information on wiring your terminal.

Remember to use the TAB key to bounce between fields, and if you get the Commands exit menu by mistake, use Cancel to return to editing this menu.

Terminal Port Configuration

This is the setup for making a terminal connect to a designated Unix host login prompt automatically.



The following fields are important:

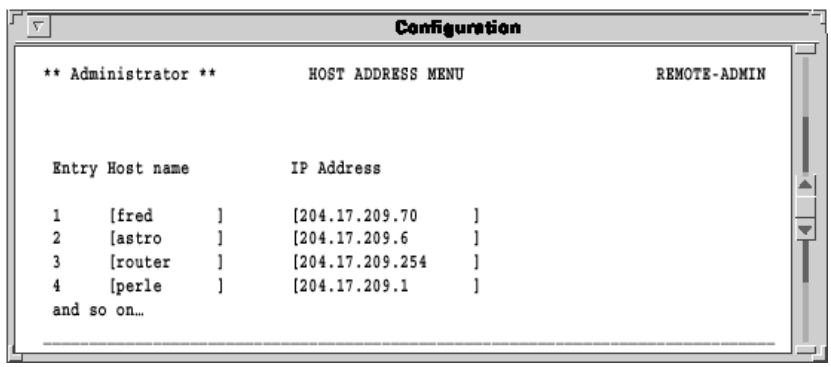
Menu option	Description
Access	Set this field to Local. This tells the terminal server port to listen for data on the RS-232 side.
Mode	With this field set to telnet, the port will operate in telnet mode (or raw for rlogin). Most systems will use telnet.
Connection	Set this field to Initiated and the port will establish a TCP/IP connection to a specified host only after receiving a <CR> on the RS-232 port. If you set this field to none, then the user of this port will see the menu system when the terminal is powered on.
Host	Use this field to define which host computer you want the port to automatically connect to when using Initiated connections. Use the host's IP address or if you setup the Host Address Menu, you can use a name.

Menu option	Description
Remote Port	This corresponds to Telnet service on the remote host and must be set to the standard 23 (or 513 for rlogin).
Monitor DSR	You can set this field to Yes if you wire the terminal's DTR signal pin 20 (DB25) to the Terminal Server's DSR signal pin 3 on the RJ45 connector (see **Appendix D Cabling** for DB25 pin assignments). When you turn the terminal off, it will reset the Terminal Server port, which tells the Unix host to kill the user's processes.

Host Table Setup

In order for your Terminal Server to connect easily to machines on the network it must know the IP addresses of the other computers. The Terminal Server can have its own internal table of IP addresses set up in the host table. This is a ‘local’ naming system only. Your Terminal Server can also use the name server utility of your Unix system (consult your Unix system manual and **Tips** on page **57**).

The Host Address Menu is accessed from the Administration Menu by selecting the host entry. The host table can contain up to 10 addresses. Each entry consists of a host name and its corresponding IP address.

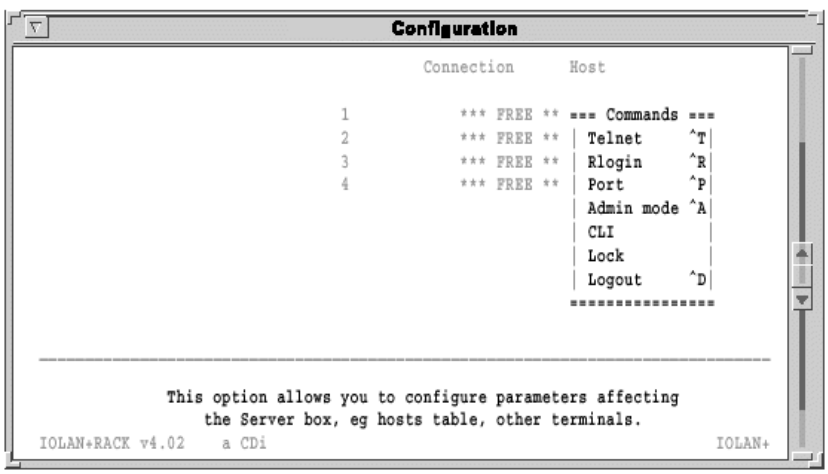


You can fill in an entry (both the name and the IP Address) for your host machines and then save the values by pressing the Enter key.

Making a Connection

If you are using initiated connections, you will not see the Terminal Server menus. Instead, you see the login prompt of the host you assigned in the host field of the Port Setup Menu.

However, if your connection field is set to None, the Connections Menu appears. You are now ready to make connections. From the Connections Menu press the Enter key on a *** FREE *** session to display the Commands menu. Select the Telnet field and press the Enter key.



This produces a pop-up menu allowing the choice of the host machines that are configured in the host table. To select a host, move the cursor down to the required name then press the Enter key. At this point the unit attempts to make a connection across the network to the indicated host using the telnet protocol.

If it succeeds, the host machine's login prompt is displayed. There may be an error in the configuration if the connection cannot be established.

> Note
>
> At this point, check the host table again for correct entries, then check the network connection and host machine you're connecting to.

While in session to the host machine, you can return to the communications server by using a hot key. This is user-defined, but defaults to ^]. Press this key and the Connections Menu is displayed. To resume your connection select the host session you were on (notice that the

name of the host is now displayed where *** FREE *** was). Press the Enter key to bring up the Connection pop-up menu, then select the Resume Connection option.

> Note
>
> If the ^] did not work, you might have a conflict with that character sequence and should check the Keys section of this port.

When logging out of your session the connection is automatically closed.

Tips

Connecting via ‘fixed ttys’

Your Terminal Server has the ability to create a ‘fixed tty’ under Unix. This is helpful for older or secure Unix applications that require a fixed location for each terminal. Consult **Chapter 9 Other devices setup**.

Multisessions on terminals/PCs

Your Terminal Server is capable of supporting multiple sessions. This allows the user to connect to all four *** FREE *** sessions with different hosts and move between them using the ^] hot key. You can also key through the screens by setting the session key (that is, If set to ^A you would bounce through the screens with a ^A1, ^A2, ^A3, ^A4.). If you are using a terminal that supports video pages such as the Wyse 60, the screens will be refreshed if you set the video pages field on the Port Menu to the number of pages supported by your terminal (for Wyse 60 = 3).

The TERM field The TERM field in the Port Setup Menu can be used to pass the terminal type information to the host. The terminal type field is local to the Terminal Server but will be passed to the host.

The TERM field can override the information being sent to the host about the type of terminal. This allows you to customise information being passed to the host. For example, a user could encode the physical location into this field (that is, tty16) and then extract that at the host end to determine which port the user has logged in on (that is, port 16).

Gateway Tables

When the host and Terminal Server are connected via a gateway router, a connection is not possible until the gateway table has been updated with the IP address of the local gateway machine. See **Gateway Menu** on page **149** in **Chapter 10 The menu interface**.

Chapter 4 Setting up dial-in modem ports

You need to read this chapter if you want to...

You need to read this chapter if you want information on creating dial-in connections with your Terminal Server product.

This chapter provides information on the configuration necessary to create dial-in connections. It includes the most simple connection such as a dial-in Unix connection, The setting up PPP ports which is how Windows ® systems dial-in (as well as Unix).

This chapter includes the following sections;

- **Introduction** on page **59**
- **Dial-in Port** on page **60**
- **The host** on page **62**
- **The modem** on page **63**
- **Client login** on page **64**
- **Tips** on page **65**.

Introduction

This chapter will review the configuration necessary to create dial-in connections. It will start with the most simple connection such as a dial-in Unix connection. The chapter then moves into setting up PPP ports which is how Windows ® systems dial-in (as well as Unix). This is very important if you are an Internet Service Provider (ISP) or a corporate site providing remote access or Internet/Intranet access.

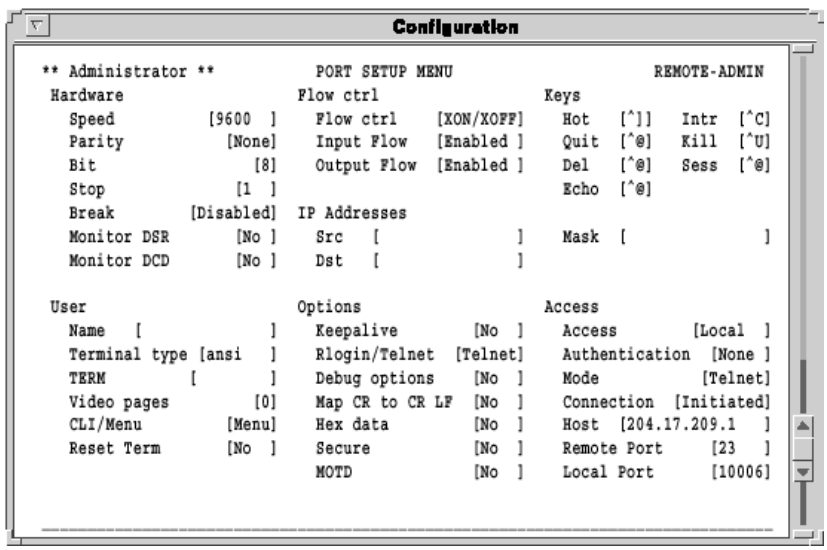
Your Terminal Server can make a very good dial-in solution for ISPs and corporate users alike by using its remote access facilities.

This chapter goes hand-in-hand with **Chapter 5 Modem authentication and logging**.

> Note
>
> In many of the modem examples, we are using PPP. You can use SLIP and CSLIP in those applications requiring these legacy modes.

Dial-in Port

The following is the port configuration for a dial-in connection, including PPP.



The following fields are important:

Option	Description
Monitor DCD	With this flag set to Yes, your Terminal Server will monitor Data Carrier Detect (DCD) - pin 8 - from the modem. As soon as your modem answers a call and establishes a carrier signal, the modem raises DCD. The terminal server will then establish a telnet/rlogin connection to a specified host. When the modem hangs up, DCD goes low and the terminal server port resets. This will also drop the connection to the host.
TERM	This field is the TERM environment variable.Whatever you type in here will be passed to the host as the TERM variable when a telnet connection is established and the user logs in.
Flow Ctrl	The modem and terminal server port should be configured to use Hardware (RTS/CTS) flow control. This will be especially important if you are using SLIP.

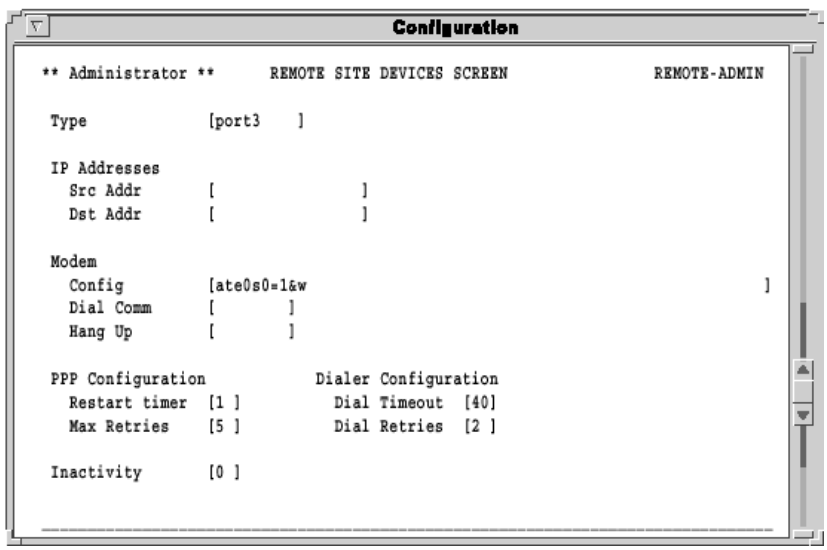
Option	Description
Dst:	This field contains the IP address the dial-in user will borrow for the PPP session. If you are using a straight forward dial-in connection for Unix, this is not required.
Mask	If using PPP, SLIP or CSLIP, this is the subnet mask that controls the range of IP addresses accessible from the port and must correspond with your network. (If used for terminals, this is not needed.)
Secure	This field is set to Yes to force the call-in user to use the Dst IP address. (su is not available in this mode.) If the Secure flag is set, the dial-in user will not be able to obtain administrative privileges. This also applies to local terminals.
Access	Set this field to Dynamic. This sets the port of the terminal server to listen for data on both the RS-232 side and the network side. If only used for dial-in, set to Local and it will only listen on the RS-232 side.
Connection	With the connection set to Dedicated, the port will automatically connect to a specified host when not doing PPP (DCD goes high on the modem).
Host	When not doing PPP, this field defines which host computer you want the port to automatically connect to. Use the host's IP address. You can also define the host in the terminal server's Host Table and just use the name.
Remote port	This corresponds to the Login (for example, rlogin) service on the remote host and must be 513 (or 23 for Telnet).
Local port	The inetd process running on the terminal server for this port is listening for TCP/IP connections on TCP port 10006.

The host

Make sure you have setup a valid user account for authentication on the designated authentication host. See **Chapter 5 Modem authentication and logging**.

The modem

You will need to configure the modem using a configuration string. To do this, go to the Remote Site Devices screen (via the Access section of the Administrative Menu). Select the UNUSED ENTRY that corresponds to the port with the modem attached (that is, third one down is port 3, etc.). You can set the type (for example, name) and the Modem Config to the required configuration string (for example, ate0s0=1&w). All other fields are default.



You will now need to kill this port (from the Administration Menu or CLI) to activate the changes and configure the modem.

The configuration string will be sent to the modem after each call, keeping the modem in sync with Terminal Server.

Client login

When the caller connects, you may want to send out a welcome message of some sort. After the user gets this message, you want him/her to enter a login and password then connect to the Host for a shell account.

Or, if it is a PPP user, they will simply start sending PPP packets at the login prompt (for example, Windows ® 95/98) and use PAP for authentication. Optionally, the dial-in user can place a P, S or C (all caps) in front of the user name at the Login prompt (this starts the corresponding protocol after successful authentication).

```
Welcome to the Internet site
login: Cflint
password:
Host authentication succeeded.
My IP Address is : 204.17.209.7
Your IP Address is : 204.17.209.210
The Subnet Mask is : 255.255.255.0
```

With this example, the Terminal Server is now in CSLIP mode, so put your PC into CSLIP mode as well. Your dialer script will have to parse out the My/Your addresses from the above message.

‘Your IP Address’ will be the address of the PC that is calling in, and ‘My IP Address’ can be the PC’s default gateway. The above procedure works for SLIP and PPP as well. However, PPP will not display the ‘My IP...’ message because the IP addresses are negotiated automatically in the IPCP layer.

With the Connection field on the Port Setup Menu set to Dedicated, if you do not specify a P, S or C in front of the user name, you will be authenticated and then connected to the host. This will leave you at a shell prompt on the Authentication host. A caller will never see Terminal Server. If Connection is set to None, you will be left at the CLI prompt (for example, IOLAN>).

Tips

Domain Name Server (DNS)

Your Terminal Server can be configured to take advantage of your network's Domain Name Server (DNS). This is important for ISPs. From the Administration Menu select server and key in the IP address of your DNS in the Name server field. You could fill in the Domain name field as well.

WINS Server

If you have a local NT server running WINS and you want dial-in clients to take advantage of that, put the IP address of the NT server in the WINS server field of the Server Configuration screen.

> Note
>
> The Windows ® 95/98 client obtains the WINS address by setting 'Use DHCP for WINS resolution'.

MOTD

A Message of the Day (MOTD) can be displayed before login. This is setup from the Server Configuration menu using MOTD and Boot host fields.

Gateway notes

If you have a router on your local network, make sure you enter this into the Terminal Server Gateway Menu.

Chapter 5 Modem authentication and logging

You need to read this chapter if you want to...

You need to read this chapter if you want information on modem authentication and logging for your Terminal Server unit.

This chapter contains information providing authentication support to validate users connecting to the serial port, and updating a host log file on connection states.

This chapter includes the following sections;

- **Introduction** on page **67**
- **User authentication/logging** on page **68**
- **The host** on page **71**
- **Logging** on page **73**
- **Tips** on page **74**

Introduction

Your Terminal Server provides authentication support to validate users connecting to the serial port, and can update a host log file on connection states. Authentication and logging is achieved by using a designated authentication host to validate users and keep connection information. This unique facility takes the burden away from the unit and more importantly allows the administrator to configure one host, rather than configuring multiple terminal servers.

Option	Description
Authentication	When the Terminal Server port has authentication set to host or both, the user is required to enter a user name followed by a password when dialed in. The user ID and password are forwarded to the authentication host for validation. By setting the authentication hosts network port to 23 or 513, this allows the user ID to be checked against the standard Unix login system (see **Tips** on page **74**). This feature also allows proprietary user validation code to be written on any TCP/IP platform by choosing another network port number.
Logging	During the Terminal Server start up, a telnet session is established to the authentication host, with the pre-defined Log Username and Logger password. Serial events like users logging in and out are recorded in the defined Log File.

Note

RADIUS is often associated, but not required, for dial-in services. RADIUS offers three major functions: authentication, logging and user services. Terminal Server can be configured to offer all of these features but without using RADIUS. This section explains how.

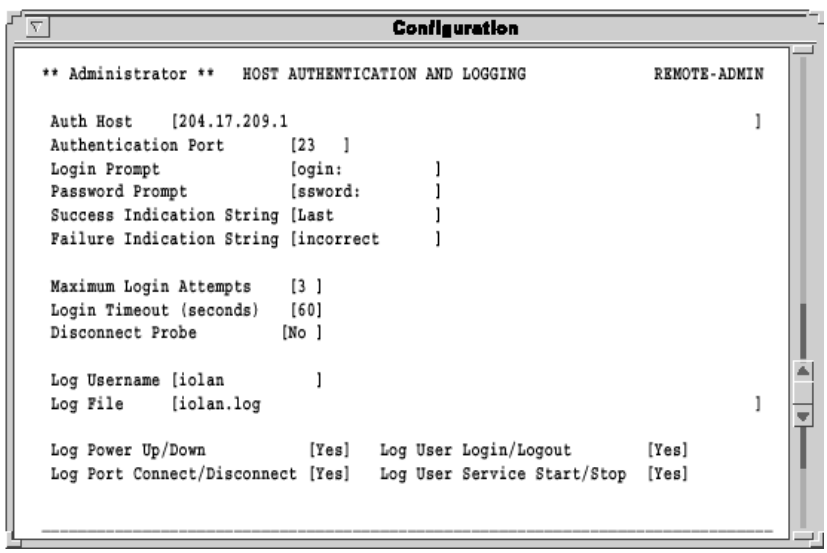
The Host Authentication And Logging menu may be accessed via the administrator from the access option in the Administration Menu.

User authentication/logging

To improve access security, the Terminal Server has a mechanism for authenticating users before allowing them access. This is accomplished by prompting the user for a Login ID and a password. The Terminal Server will then attempt to login to a specified host using that ID and password. If successful, the user is authenticated and allowed access. Otherwise, the call is dropped. Your Terminal Server will also log events such as logins, logouts, connections and disconnections, and power ups.

This feature is enabled when you set the Authentication field to host in the Port Setup Menu.

The following is the host authentication setup (via the Access section of the Administration Menu):



The following fields are important:

Option	Description
Auth Host	The IP Address/Name of the host that the Terminal Server attempts to login to for authenticating users.
Authentication Port	The TCP service to be used for authenticating users. Normally this is set to 23 for Telnet.
Login Prompt	The string used by the Terminal Server to know when to send the login ID. Set this field to ogin:. Leave out the first letter as some systems use a 'L' and others use a 'l' as the first letter.
Password Prompt	The string used by the Terminal Server to know when to send the users password. Use 'ssword' as depicted above.
Success Indication String	The string used by the Terminal Server to determine if the login ID and Password were valid and the login process was successful. Normally you will see the string 'Last' after successfully logging in.
Failure Indication String	The string your Terminal Server will look for to determine that the Login ID or Password were invalid. You will normally see the word 'invalid' or 'incorrect' as part of the failure message from the host.
Maximum Login Attempts	The number of login attempts your Terminal Server will allow the user to make before dropping the call.
Login Timeout	This defines the amount of time in seconds the Terminal Server will wait for the user to provide a login ID and password before dropping the line.
Disconnect Probe	This option determines whether authentication probe logins will be terminated on completion of authentication.
Log Username	The User ID your Terminal Server will use to log in to the authentication host and log messages. This user needs to be at a shell prompt to 'cat' messages to the log file. The password for the log user is set up under the Terminal Server Administration Menu -Change option. Then choose the Logger option and enter the log user's password as defined on the host. You will have to enter this password twice. (See **Tips** on page **74**.)
Log File	The filename the log user will send itsmessages to. Normally this will go to the log user's home directory.
Log Power Up/Down	The Terminal Server will log when it is powered up and rebooted.
Log User Login/Logout	The Terminal Server will log when a user logs in and out of a port on Terminal Server.

Option	Description
Log Port Connect/ Disconnect	The Terminal Server will log when someone connects to and disconnects from a port on Terminal Server.
Log User Service Start/ Stop	The Terminal Server will log a PPP, SLIP or CSLIP service when started on the port.

The host

Basic authentication

Your Terminal Server will need to login to the authentication host with the log user name defined on the Host Authentication And Logging screen. Therefore, you need to create an account to be used by Terminal Server (avoid csh shell). Make sure the user can log in successfully. Also, make sure the user is not prompted for any input and ends up at a shell prompt.

User services authentication

This is used to provide services based upon the dial-in user's name.

For example, user Mark always telnets to a specific IP address or user Alan needs to dial-in and establish a PPP connection using a static IP address. This is accomplished by using a PERL script which parses a RADIUS database. The PERL script (RADparse) is on the CD or our website.

RADIUS is the TCP/IP protocol used for authenticating remote dial-in users. Although Terminal Server does not use RADIUS, a Perl based utility capable of using standard RADIUS databases is available.

Otherwise, you can execute our PERL script during the user's login. Under Unix, this script is started from the etc/profile.

You then need to create a user database file. This is a sample file.

```
# Example of a PPP user with static address
alan Password
Framed-Protocol = PPP
Framed-Address = 204.17.209.1

# Example of a user with access to Terminal Server
CLI/Menu
techman Password
User-Service-Type = Shell-Use

# Example of a telnet user
mark Password
User-Service-Type = Login-User
Login-Host = 208.24.183.1
Login-Service = Telnet
```

```
# Everybody else gets PPP with a dynamic address
DEFAULT Password
Framed-Protocol = PPP
```

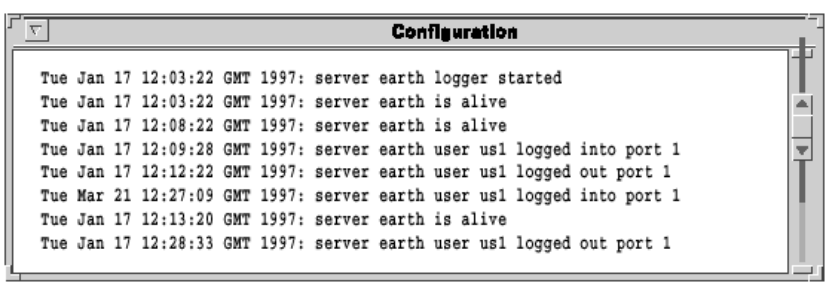
> Note
>
> When using advanced authentication, make sure the Success Indication String in the Host Authentication And Logging menu is set to userdefined.

Logging

A log file can be updated on the authentication host to record when a Terminal Server is powered up, rebooted, and users and ports are connected and disconnected. This information is of particular importance to administrators who need to record users logging in and out. In addition, when the logger is enabled the Terminal Server completes a time stamp every 5 minutes to record that the Terminal Server is still active. This allows an administrator to gain an accurate record of events.

See **User authentication/logging** on page **68** (via the Access section of the Administration Menu).

When the Terminal Server is powered up a Telnet connection is established to the authentication host with the Logger user name. The Terminal Server records users logging in and out of the log file access.log. The logger only connects at Terminal Server start-up time and the connection stays open until the unit is reset. The Terminal Server checks the log TCP connection every 60 seconds. The logger may be restarted via the kill command by adding two to the number of ports on your server (for example, use four for an Terminal Server2, six for an Terminal Server4, ten for an Terminal Server8, eighteen for an Terminal Server16). If the host authentication succeeds, but logger fails to log events, then the port connection is dropped.



Tips

Windows ® notes

Authentication of Windows NT ® requires a telnet daemon. Check the Windows ® section of our website for the latest Windows ® telnetd software. You will need to set up your users on Windows NT ® through this software.

Logging on Windows NT ® also requires a utility called log_it.exe. If the Windows NT ® login user id is ‘logger’, enter it into the Terminal Server as Nlogger so that the Terminal Server will know to use the log_it.exe utility.

Also, on the Host Authentication And Logging menu, change the Terminal Server Success Indication String to read, Microsoft instead of Last.)

Unix notes

For LINUX users, edit the file /etc/motd and put the word ‘Last’ in it. This will agree with the standard setup of the Host Authentication And Logging menu’s Success Indication String.

Chapter 6 Dialout modem ports setup

You need to read this chapter if you want to...

You need to read this chapter if you want information on setting up modem ports for your Terminal Server product.

This chapter provides on setting up modem ports for your Terminal Server product. Dial-out ports can be just a simple Unix outbound cu call or your Terminal Server can act as a dial-out router to facilitate Internet PPP requests.

This chapter includes the following sections;

- **Introduction** on page **76**
- **Configuration** on page **77**
- **The host** on page **78**
- **Routing** on page **79**
- **Remote Access Systems** on page **80**
- **Remote site devices** on page **83**
- **Tips** on page **84**.

Introduction

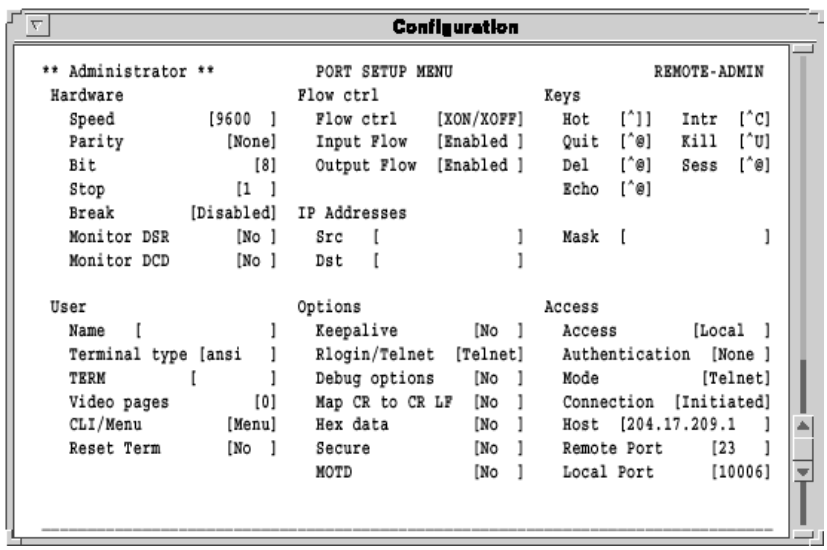
Dial-out ports can be just a simple Unix outbound cu call or your Terminal Server can act as a dial-out router to facilitate Internet PPP requests.

As a dial-out router your Terminal Server automatically establishes a PPP/SLIP/CSLIP link to that site. Then drops the call after a preset period of inactivity. This dial-on-demand feature is automatic. Your Terminal Server will place the call when local TCP/IP traffic needs to be routed to a configured remote site.

If not using dial-out routing, you will need a COMPORT redirector such as ioland. The CD has the ioland utility if you are using Unix. Please load the appropriate binary onto your system. If you can not find the correct binary, please compile the ioland.c source code for your system (see your Unix manual).

Configuration

The Port Setup Menu should be set up as follows for both simple dial-in connections and PPP/SLIP connections.



The following fields are important:

Field	Description
Access	Set the Access field to Dynamic (dial-in or out) or Remote (dial-out only).
Monitor DCD	With this flag set to Yes, the terminal server will monitor the modem signal Data Carrier Detect (DCD) - pin 8. When the modem hangs up, pin DCD from the modem goes low and the terminal server port will reset.
Flow Ctrl	The modem and terminal server port should be configured to use Hardware (RTS/CTS) flow control. This will be especially important if you are transferring binary files.
Mode	Set this field to raw.

The host

For dial-out connections on Unix

If you have not already loaded ioland onto your system, do so now (see CD). For more information on ioland see **Chapter 9 Other devices setup**. In it's simplest form, at the superuser prompt you would run the following command in Unix:

```
ioland -h <server-name> 10006 <device-name>
```

This will start the ioland process and allow you to specify a device-name in /dev that is linked to a pseudo tty. This pseudo tty works just like a regular tty with the following exception: you cannot set physical attributes such as baud rate, parity and flow control as these are handled by the terminal server. If you plan to use communication software on the Unix host such as cu or uucp you should refer to your Unix manual for additional help.

For dial-out connections on Windows ® systems

Check our website for the latest information on dial-out connections (under the Windows ® support).

Routing

For dial-out routing, you must have the proper routing entry on all hosts in your local network that will communicate with the remote site. In the case of a Unix system, you must make an entry similar to the following (please check your Unix manual for the proper syntax of the route command):

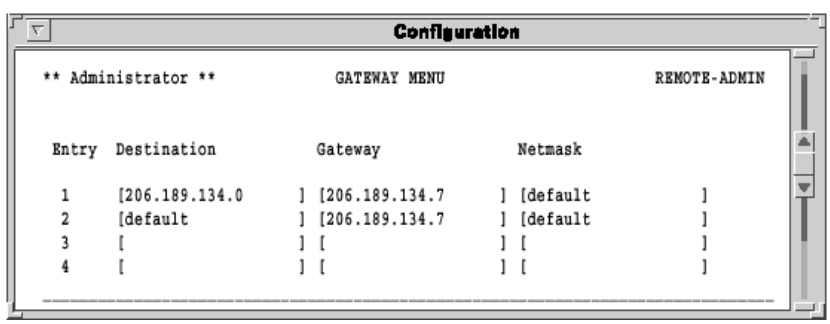
For a single host at the remote site:

```
route add <remote-ip-addr> <IOLAN-ip-addr> 2
```

For multiple hosts at the remote site:

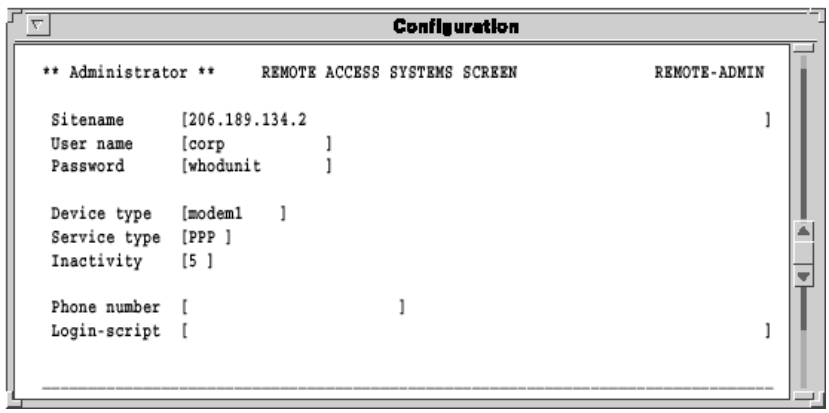
```
route add net <remote-net-addr> <IOLAN-ip-addr> 2
```

The Terminal Server will dial into another piece of hardware, log into that hardware and start a PPP session. Then the local Terminal Server will act as a router and forward all IP traffic destined outside its local network. In other words, the Terminal Server will 'auto-dial' the Internet and act as the router. In this example, the local network is: 206.131.227.0, the ISP's network is: 206.189.134.0, the ISP's equipment that you are dialing into is another Terminal Server (206.189.134.7) and the local Terminal Server is: 206.131.227.5. The Terminal Server gateway entries look like this:



Remote Access Systems

This screen is used to define a remote system (up to 16 entries per unit), a phone number, login script, etc. There are a lot of similarities between this screen and the UUCP systems file under Unix.



The following fields are important:

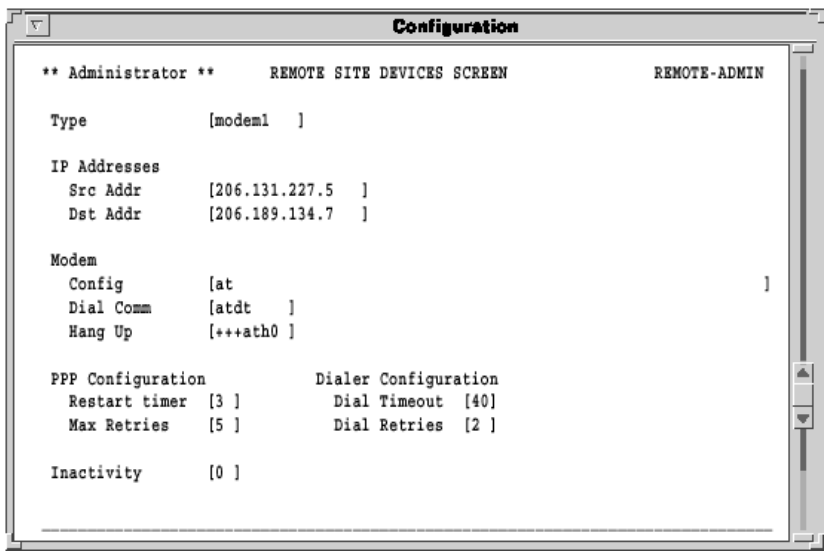
Field	Description
Sitename	The IP name or IP address of the remote site Terminal Server will be calling.
User name	The user name required by the remote system for logging in. You may use the \u in your login script in lieu of the full name.
Password	The above user name's password as required by the remote system. You may use the \p in your login script in lieu of the full password.
Device type	The name of the modem device as defined in the Remote Access Systems Screen. You may have several ports setup with the same device type, and the dialer will use the first available. If a device for dialling out is not available, the Terminal Server will return an ICMP 'host unreachable' message (ICMP type 3 code 1).
Service type:	This specifies which protocol will be used when the link is established to the remote site. Choices are PPP, SLIP and CSLIP.
Inactivity	The period (in minutes) of inactivity on the SLIP/ PPP link before the port drops the call automatically. Setting this field to 0 turns the timeout feature off.
Phone number	The phone number of the remote system. Note that the '\' may be used as a delay. For example, a phone system that requires a 9 followed by a four-second delay before getting an outside line would require an entry like 9\4-2145551234.
The following characters are ignored '(', ')', '-', '.'	when included as part of the number.
Login-script	The chat script that will be used to login to the remote system. It takes the form of the usual Send/Expect chat script you may already be familiar with. If no script is defined, this step is skipped (for example, hardwired connections). There are a few special characters used by the Terminal Server as described below: "" expect nothing (for example, the Terminal Server starts the chat script) \r send a carriage return \n send new-line \u user name (sends the username from the User name field). \p password (sends the password from the password field). \1-\9 delay for number of seconds. \s space (Substitute this instead of a <space> value). \t phone# (sends the telephone number field). \d send the modem's dial command \\ escapes to '\'. \b send a break.

Dial-out PAP Authentication

If a dial-out script is not used but a username and password are defined, your Terminal Server will send a PAP packet after establishing a PPP link and use the username and password defined for the remote site.

Remote site devices

This screen is used to define/setup the modem device. There are a lot of similarities between this screen and the UUCP devices file under Unix. It is possible to assign several ports the same device name, and the dialer daemon will automatically use the first available port. It is also possible to have these ports do ‘double-duty’ and serve as regular dial-in ports for dumb terminal access, SLIP or PPP in addition to the dial-out capability.



The following fields are important:

Field	Description
Type	The name of the modem assigned to a specific port. It is referenced from the Remote Access Systems Screen in the Device type field.
Dst Address	The address of the remote system your Terminal Server is calling into.
Config	The modem’s configuration string. There are a few examples at the end of this document. Note: Leave this field blank for directly connected devices.
Restart timer	Amount of time in seconds before the Terminal Server retransmits PPP options.

Field	Description
Max Retries	Number of option retries before dropping the line.
Dial Timeout	Number of seconds to wait for the modem to establish link and respond.
Dial Retries	Number of times to attempt a connection to the remote site before giving up.

Tips

Hunt groups You can setup several modems and use the same name for each group under Remote Site Devices. The Terminal Server will use the first available modem defined in Remote Site Devices, which if busy will default to the next available.

Chapter 7 Vmodem (Virtual modem)

You need to read this chapter if you want to...

You need to read this chapter if you want an overview of the Terminal Server products Virtual modem feature.

This chapter provides information about the Vmodem feature of the Terminal Server, which provides “modem like” communication between two Terminal Server units on a network. This feature behaves like two modems connected across a telephone line.

This chapter includes the following sections;

- **About Vmodem (Virtual modem)** on page **86**
- **Configuring ports to use Vmodem** on page **87**
- **Setting/Modifying up Vmodem responses** on page **92**
- **Vmodem AT Commands** on page **93**.

About Vmodem (Virtual modem)

Vmodem is a feature of the Terminal Server, which provides “modem like” communication between two Terminal Server units on a network. This feature behaves like two modems connected across a telephone line.

Typically, you use the Vmodem feature when you have multiple devices communicating with a central site.

Vmodem allows you to achieve this using a single Terminal Server unit at each end of the network without having to use multiple modems.

You use Vmodem because you want to avoid having to use multiple modems with the associated costs of calls and connections.

You use this feature by logging into the Terminal Server via a terminal or telnet. You then enable and configure the Vmodem feature on the ports you want to use. You then connect your remote devices to the Vmodem ports on the Terminal Server units.

Configuring ports to use Vmodem

The Vmodem feature has two modes, Normal and Dial on DTR.

- In normal mode, the Vmodem ports behave like a modem using basic AT commands to connect and disconnect.
- In Dial on DTR mode, the unit will automatically connect to a pre-configured destination.

Configuring ports to use Vmodem in Normal Mode

Carry out the following on all the participating Terminal Server units;

1. Login to your Terminal Server unit using either serial link or telnet as required.
2. Within the CONNECTIONS MENU now displayed, select a FREE connection and press the Enter key.
3. Select Commands > Admin mode and press the Enter key.
4. Select ADMINISTRATION MENU > Password and press the Enter key.
5. When prompted, enter the password and press the Enter key.

   The ADMINISTRATION MENU is now updated to show additional features available in administration mode only.

6. In the updated ADMINISTRATION MENU; Select Port and press the Enter key.

   At the Port prompt now displayed, type in the port to be configured for Vmodem and then press the Enter key.

7. In the PORT SETUP MENU; Highlight the Access field and press the Enter key.
8. Select Access >Values and press Enter key.
9. Select Access > VModem and press the Enter key.

   You are now returned to the PORT SETUP MENU.

10. If the AT command +++ATH is required to hang up a connection;
    a. In the PORT SETUP MENU now displayed;
    b. Set the Mode field in the Access area to Telnet.
    c. Otherwise, set the Mode field to RAW.
11. Within the Hardware area, set the Monitor DSR field to No. Leave all other fields at their default settings.
12. In the PORT SETUP MENU screen; Press the Enter key.

    When prompted, select Save and exit.

    The ADMINISTRATION MENU is now displayed.

13. Press the Escape key to go back to the CONNECTIONS MENU.
14. In the CONNECTIONS MENU;
    a. Select a FREE connection and press the Enter key.
    b. Select Commands > CLI.
15. Connect the devices required to the Vmodem port on the Terminal Server using the appropriate cable.
16. Repeat this procedure for all ports you want to configure to use Vmodem.

Making a Call using Vmodem in Normal Mode

Using Vmodem, telephone numbers are replaced by the IP address and TCP port of the Vmodem port you are calling.

1. To place a call using the device attached to a Vmodem port, the ATD sequence would be:

   ATD<IP address><Port>

   Where:

   IP address is the IP address of the Terminal Server unit that you are calling. where each number is represented by three digits (padded using zeros where necessary) with no separating dots.

   Port is the local TCP port of the Vmodem port on the Terminal Server unit you are calling, (By default the TCP port is 10000 plus the number of the serial port using Vmodem.
   For example, Port 12 would become 10012).
   For example, to connect to a host Terminal Server with an IP address of 196.65.144.236 and serial port 4 configured as Vmodem normal mode, the ATD sequence would be;

   ATD196065144236100004 (This is not echoed by the port)

   The Vmodem now returns a numerical or text string to indicate either a successful or failed connection.

2. You can configure how this indication is displayed see the appropriate section within this note.

Disconnecting a Call in Vmodem Normal Mode

To disconnect a call, the sequence +++ATH is sent to the Vmodem port.

Configuring Vmodem to use Dial on DTR mode

You use Dial on DTR mode because you want your device to dial a preconfigured number automatically when DTR is raised by the device.

To configure your port, proceed as follows;

1. Login to your Terminal Server unit using either serial link or telnet.
2. Within the CONNECTIONS MENU now displayed, select a FREE connection and press the Enter key.
3. Select Commands > Admin mode and press the Enter key.
4. Select ADMINISTRATION MENU > Password and press the Enter key.
5. When prompted, enter the password and press the Enter key.

   The ADMINISTRATION MENU is now updated to show additional features available in administration mode only.

6. In the updated ADMINISTRATION MENU;
7. Select Port and press the Enter key.
8. At the Port prompt now displayed, type in the port to be configured for Vmodem and then press the Enter key.
9. In the PORT SETUP MENU;
   a. Highlight the Access field and press the Enter key.
   b. Select Access >Values and press Enter key.
   c. Select Access > VModem and press the Enter key.

   You are now returned to the PORT SETUP MENU.
10. If the AT command +++ATH is required to hang up a connection;
11. In the PORT SETUP MENU now displayed;
12. Set the Mode field in the Access area to Telnet. Otherwise, set the Mode field to RAW.
13. Within the Hardware area, set the Monitor DSR field to Yes to enable Dial On Dtr mode.
14. At the Host field enter the HOST Terminal Server IP address of the Terminal Server to be auto-dialled.
15. In the Remote port field enter the TCP port of the serial port on the Terminal Server to be auto-dialled.

    (Note: this value is the Local port setting on the Terminal Server to be auto-dialled which by default will be 10000 plus the serial port number of the Vmodem port to dial.)

16. Leave all other fields at their default settings.
17. In the PORT SETUP MENU screen;
    a. Press the Enter key.
    b. When prompted, select Save and exit.

The ADMINISTRATION MENU is now displayed.

c. Press the Escape key to go back to the CONNECTIONS MENU.

18. In the CONNECTIONS MENU;

    a. Select a FREE connection and press the Enter key.

    b. Select Commands > CLI.

19. Connect the devices required to the Vmodem port on the Terminal Server using the appropriate cable.

20. Repeat this procedure for all ports you want to configure to use Vmodem.

Making a Call using Vmodem in Dial on DTR Mode

Using Vmodem in Dial on DTR mode will cause the host IP address and remote TCP port number to be called automatically on detection of the DTR signal being high.

1. Raising DTR (connected to DSR on the Terminal Server Vmodem port) will make a connection to the pre-configured remote Terminal Server unit.

Disconnecting a Call in Vmodem Dial on DTR Mode

1. Dropping DTR (connected to DSR on the Terminal Server Vmodem port) will cause disconnection, typing +++ATH will produce the same result.

Setting/Modifying up Vmodem responses

The default responses for failure/success of a connection, may be customized.
To configure the Vmodem responses, proceed as follows;

1. Login to your Terminal Server unit using either serial link or telnet as required.
2. Within the CONNECTIONS MENU now displayed press the Enter key and select;.
   Commands > Admin mode and press the Enter key.
   ADMINISTRATION MENU > Password and press the Enter key.
3. When prompted, enter the password and press the Enter key.

   The ADMNINISTRATION MENU is now updated to show additional features available in administration mode only.

4. In the updated ADMINISTRATION MENU, select:
   Access and press the Enter key.
   Access > Vmodem and press the Enter key.
5. In the VMODEM SETUP screen now displayed, set the following fields if required;

   Success Indication String: Sent to the device when a connection succeeds.
   If no string is entered, then the string “CONNECT” will be displayed with the connecting speed, for instance “CONNECT 9600”.

   Failure Indication String:Sent to the device when a connection fails.
   If no string is entered, then the string “NO CARRIER” will be displayed.

   Suppress Result Codes (Yes/No):If set to no, connection success/failure indication strings are sent to the connected device, otherwise these indications are suppressed.

   Result Code Style (Verbose/Numeric):
   If set to Verbose, then string result codes are sent to the connected device.
   If set to Numeric, then the following characters are sent to the connected device:

   ‘1’ Successfully Connected
   ‘2’ Failed to Connect
   ‘4’ Error

Vmodem AT Commands

Ports configured for Vmodem operation interpret the following AT command codes.

Code	Description
+++ATH	Disconnect and hang-up a connection.
ATQ0	Enable connection responses for the duration of the session.
ATQ1	Suppress connection responses for the duration of the session.
ATV0	Selects numeric results codes for the duration of the session.
ATV1	Selects verbose results codes for the duration of the session.

All other AT sequences are accepted, but ignored by the Vmodem port.

Chapter 8 Printing

You need to read this chapter if you want to...

You need to read this chapter if you want information on printing from your Terminal Server product.

This chapter provides information about the three methods of printing from your Terminal Server: ioland, LPD, or RCP. ioland is the recommended method, however this will depend on your application and operating system.

This chapter includes the following sections;

- **Introduction** on page **95**
- **Using ioland** on page **96**
- **Using LPD** on page **99**
- **Using RCP** on page **105**.

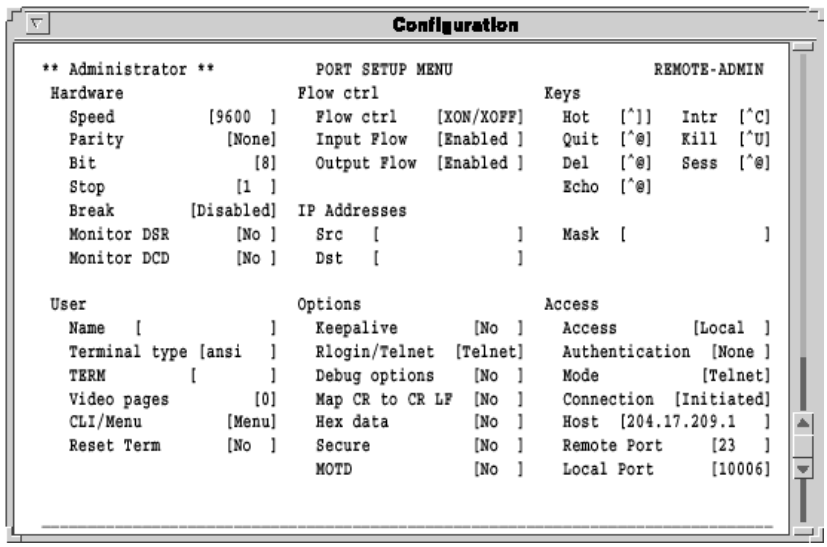
Introduction

There are three methods of printing from your Terminal Server: ioland, LPD, or RCP. ioland is the recommended method, however this will depend on your application and operating system.

Method	Description
ioland	ioland provides a pseudo TTY interface to Unix print spoolers (not available for Windows ®). This software and the binaries associated with it are available from the CD provided with the unit or from the website.
LPD	LPD is the 'line printer daemon' protocol supported by mmost operating systems including Windows ® and Unix (for example, SCO, AIX, DG/UX, HP-UX, Linux, Solaris, etc.) for an LPD spooler for Windows ® 95/98 see our website.
RCP	RCP is 'remote copy printing' and available on Unix systems. It requires a special interface script also found on the CD.

Using ioland

We suggest you use the ioland utility on the CD provided. The ioland utility can be used for Unix printing only. Ioland is a Unix tty port redirector. For non-UNIX applications use LPD, see **Using LPD** on page **99**.



The following fields are important:

Field	Description
Flow ctrl	Set your Terminal Server port flow control to Hardware. Then set your printer to use 'DTR Pacing' or 'Hardware' or 'Ready/Busy' flow control. Use the RS-232 printer cable pinout shown in **Appendix D Cabling**.
Access	Set this field to Remote. This sets the port of the terminal server to listen for connections coming from the network. There will be an INETD process running on the terminal server that does the listening.You can check on the status of this process by looking at the Netstat screen of the terminal server's Statistics menu (or show net from the CLI prompt).
Mode	Set this field to Telnet. This puts the port of the terminal server in Telnet mode, which will ensure that EOF is properly negotiated before closing down the TCP/IP connection, otherwise the tail end of a print job could be lost.
Local port	The INETD process running on the terminal server for this port is listening for TCP/IP connections on TCP port 10006.

If you are already familiar with ioland, all you have to do for the above configuration is:

```
ioland -T <server name> 10006 <device name>
```

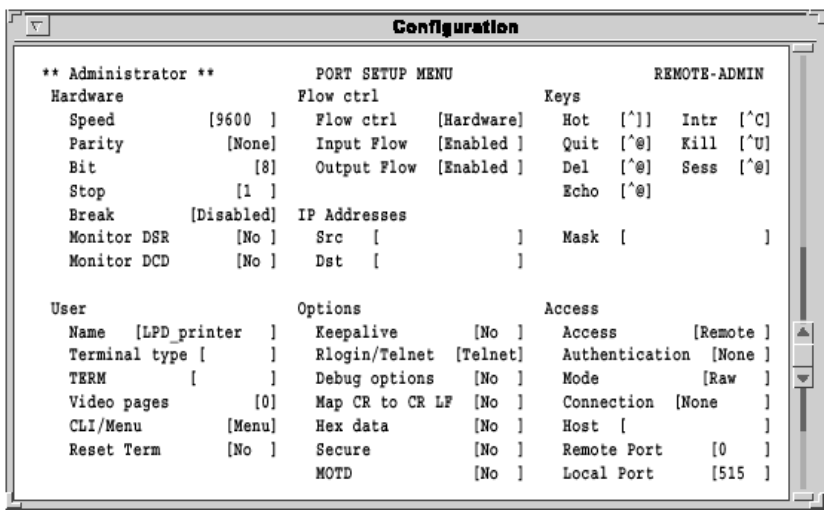
This will start ioland process and create a device in /dev. If you are not familiar with the ioland program, **Chapter 9 Other devices setup**.

> Hint
>
> Hunt groups are supported on the Terminal Server for printing. To use this, use the same number in the Port Setup local port field (for example, 1006).

Using LPD

Your Terminal Server can be setup for receiving print jobs via LPD and this is a very simple method. It works for both Windows ® and Unix systems.

Configuration



The following fields are important:

Field	Description
Flow control	Set your Terminal Server port flow control to Hardware. Then set your printer to use 'DTR Pacing' or 'Hardware' or 'Ready/ Busy' flow control. Use the RS-232 printer cable pinout shown in the Cabling Guide (Appendix C), as this will save a print job if the printer is turned off or the cable becomes detached.
Name	The LPD client, as a reference to the printer, will use what you assign here. This is the printer queue name on the Terminal Server.
Access	Set this field to Remote. This sets the port of the terminal server to listen for connections coming from the network. There will be an INETD process running on the terminal server that does the listening. You can check on the status of this process by looking at the NETSTAT screen of the terminal server's STATS menu (or show net).
Mode	The port of the terminal server will operate in a raw TCP/IP mode.
Local port	The INETD process running on the terminal server for this port is listening for TCP/IP connections on TCP port 515 (this is the LPD service number).

The client is the machine that contains the file to be printed and may be running one of a range of operating systems and applications. The client must support LPD, Unix systems normally include a version of LPD and there are a number of TCP/IP applications for DOS/ Windows ® that also support LPD.

When printing via LPD the client refers to the printer by IP address (or the name associated with this address from the host table) and printer name or queue name. This may take one of the following forms:

- The name of the terminal server and no queue name or port number. This will cause the print job to be printed on the first available LPD port on the terminal server of this name. The Name field in the Port Setup Menu does not need to be set.
- The name of the terminal server followed by a port number. For example if the queue name is server_name9 (or server_name09) then serial port 9 will receive the print job. Please note that in this example, the Name field in the Port Setup Menu need not be set.
- The printer name as set in the Name field of the Port Setup Menu. More than one serial port may have the same name allowing the server to create a hunt group of printers. The first available port to match that queue name will receive the print job.

A special feature of LPD with terminal servers is the ability to do carriage-return and line feed mapping at the server. This is accomplished by having a + appended to the client queue name and is valid for all of the above methods of access. Alternatively, you may enable the CR to CR LF mappingoption for the port.

> Note
>
> There is a maximum limit of 30 LPD connections per server, which may be distributed to all of the available LPD ports as required. If the maximum is exceeded then the request is rejected and the connection is closed.

LPD printing from DOS/Windows ®

At present it is possible to print from Windows ® or DOS although this will normally be accomplished via a separate application program like PC/TCP or Netmanage Chameleon. The new versions of Windows ® type operating systems either have or intended to have TCP/IP built into the operating system. Windows NT ® has a built-in LPD utility, and there are shareware packages on the Internet for Windows ® 95/98 (check our website).

The documentation for each application or operating system should allow users to configure and use it with the Terminal Server. The obvious advantage of using LPD to print is that the server can be used to connect a printer that will be shared between both DOS/Windows ® and Unix machines.

Under Windows ® the printer will be available from within other applications via the File option of the Windows ® menu bar.

The actual printer will be referenced by the Name of the terminal server serial port or, by the terminal server and port number in the same way that Unix uses the Name.

The server IP address should be included in the Host table before trying to setup the actual printer port.

LPD Printing from BSD Unix and Linux

This section should give you some idea of how to set-up printing via LPD on a Unix host. However, this will not be universally true as different versions of Unix have different configuration requirements. You may also wish to consult your Operating System documentation before attempting to add LPD.

The Unix host should have a printer database, for BSD and Linux type systems this will be the file /etc/printcap and there should be an entry within this file for the server's LPD port that looks something like the following:

```
#term_serv LPD Printer on serial port 16
Laser1|IOLAN LPD printer 16:\

:rp=LPD_printer:rm=term_serv:lp=:sf:\
:sd=/usr/spool/LPD/LPD_printer:\
:lf=/usr/spool/LPD/term_serv16/log:
```

Printing could then be accomplished using the following command:

```
lpr –PLaser1 <file>
```

A limitation of printing with LPD on the terminal server is that no formatting of text (apart from the + operation) can be carried out by the terminal server firmware. This is due to the lack of a spooler utility in the terminal server and the data being forwarded directly to the serial port.

To overcome this the local host must perform all of the necessary changes and then send these to the terminal server. Defining a printer queue as in the previous examples can do this.

If filtering or formatting is required then a local linking print queue needs to be created. This would be something like the following:

```
# Lcl q to link to term_serv LPD Printer on port 16
link-Laser1| IOLAN LPD Printer 16:\
:lp=/dev/null:sf:sd=/usr/spool/LPD/Laser1:\
:lf=/usr/spool/LPD/LPD_printer/log:\
:of=/etc/IOLAN/link-Laser1:
```

The shell script output file link-Laser1 has the contents:

```
#!/bin/sh
lpr –PLaser1
```

This would be sufficient to print a header page and perform form feeds. If a specialised filter program is required for something like a plotter then the script may look something like the following:

```
#!/bin/sh
/usr/local/filter '$@' | lpr -PLaser1
```

LPD Printing from SYS V Unix

Here is an example for setting up the System V spooling system (for example, Linux, Solaris, etc.) to print to the Terminal Server LPD daemon. This assumes that you will print to a port configured like the example above on an Terminal Server called term_serv.

lpsystem -t bsd term_serv lpadmin -p Laser1 -s term_serv If the terminal server is not defined in the /etc/hosts file you may not get an error message from either the lpsystem or lpadmin commands, but the printer will not print.

If the lpsystem command is not performed, the lpadmin command will return an error indicating that the system named in the -s parameter does not exist even though the system is listed in the /etc/hosts file.

> Note
>
> Although it is possible to create a printer spool on the Terminal Server, UNIX lpd queues only print one job at a time. The host will wait for one job to complete before spooling the second so all jobs will go to the same queue and print from the same port.

LPD printing from AIX

Use SMIT to configure remote printer.

LPD printing from HP/UX

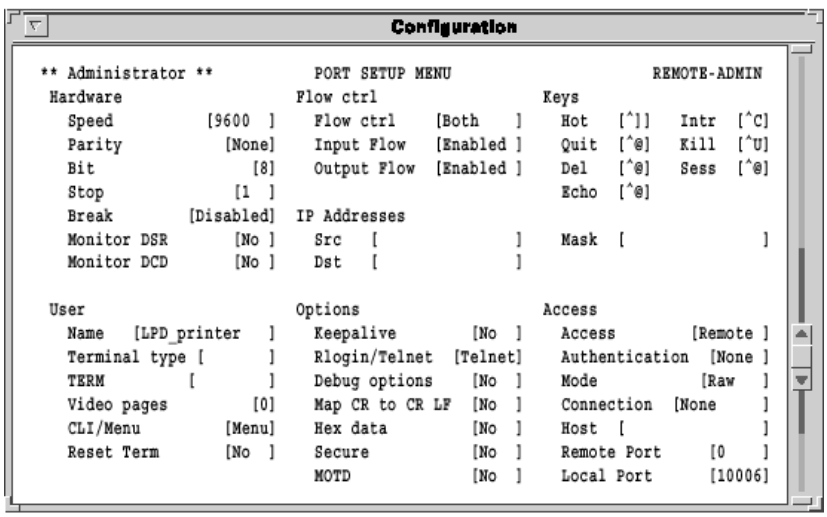
Use SAM to configure remote printer.

> Hint
>
> Hunt groups are supported on the Terminal Server for printing. To use this, use the same queue name in the Terminal Server Port Setup name field.

Using RCP

RCP is used as an alternative option (where LPD and ioland are not available). It is a Unix only command set. A script is provided on the CD for RCP.

Configuration



The following fields are important:

Field	Description
Flow ctrl	Set your Terminal Server port flow control to Both. This will invoke both Hardware (RTS/CTS) and XON/XOFF flow control on the Terminal Server. Then set your printer to use XON/XOFF. Use the RS-232 cable pinout described in **Appendix D Cabling**, as this will stop a print job if the printer is turned off or the cable becomes detached.
Access	Set this field to Remote. This sets the port of the terminal server to listen for connections coming from the network. There will be an INETD process running on the terminal server that does the listening. You can check on the status of this process by looking at the NETSTAT screen of the terminal server's Statistics Menu (or show net from CLI).

Field	Description
Mode	The port of the terminal server will operate in a raw TCP/IP mode.
Local port	The INETD process running on the terminal server for this port is listening for TCP/IP connections on TCP port 514 (this is the RCP service number).

The Host

On systems where LPD or a binary for ioland is not available, or is found to be unreliable due to limitations in the OS, RCP provides a useful, if limited, alternative method for printing. The port/group of ports must be configured to listen to the RCP port, which is port 514. Users can then copy files to the server using the following command syntax:

rcp <file> <server>:tty [port #]

It is worth noting that the RCP will fail if the port (or all the ports in the hunt group) is in use when the RCP command is attempted. If you wish to use RCP as part of a System V print spooler script, it is essential that the script checks the return status of the RCP command.

Using RCP with Unix System V line printer spoolers.

1. Log in as root and create a print queue for the printer with /dev/null as the device port. For example, create an HP LaserJet printer queue via the command:

   /usr/lib/lpadmin -hpjet -v/dev/null -mHPLaserJet

   Do not accept or enable the printer at this stage.

2. Go into the directory containing the interface scripts for all printers. This is normally found in:

   /usr/spool/lp/admins/lp/interfaces (Rel 3 Unix).
   /etc/lp/interfaces (Rel 4 Unix).
   /usr/spool/lp/interfaces (XENIX).

3. Find the interface shell script for this printer and copy it to a file with the suffix '.orig'. using the example: cp hpjet hpjet.orig
4. Copy the Server RCP shell script from the TSSD support disk to the interface script, e.g:cp /etc/xxxx/src/xxxx.rcp hpjet
5. Having created the hpjet file set the permissions to allow execution of the script, e.g: chmod a+x hpjet
6. Edit the interface script and insert the desired server name and port number. For example, if the name is 'iceland' and the printer is attached to port 8 (numbering from 1 to 16). Then the line:

   rcp $TMP <server name>:tty<port number>

   becomes:

   rcp $TMP iceland:tty8

   Some Unix systems may require the full pathname of the 'RCP' command. For example:

   /usr/ucb/rcp $TMP iceland:tty8

7. Activate the printer for use, e.g:

   /usr/lib/accept hpjet enable hpjet

8. Set up the Terminal Server port for RCP printing by changing the Local Port field in the Access section of the Port Setup Menu to 514.

RCP printing on a spooler system based on BSD Unix

Currently, the RCP printing utility will not work if the of filter is used in conjunction with any other filter.

1. Log in as root and create a print queue for the printer with /dev/null as the device port. For example, create a printer queue by placing this record in /etc/printcap:

   rcp Printer to IOLAN port 8
   IOLAN8|IOLAN rcp Printer:\
   :lp=/dev/null:\
   :sf:\
   :sd=/usr/spool/LPD/IOLAN8:\
   :lf=/usr/spool/LPD/IOLAN8/log:\
   :if=/etc/xxxx/hpif:

2. Go into the directory containing the desired text filter program intended for the if field. If there is no filter required for this queue then create a dummy filter program which calls the cat command with no arguments.
3. Link the generic filter program to a file with the suffix '.orig'. This generic filter program may be in use by other printer queues and so is left untouched. Using the example:

   ln -s <filter-name> /etc/xxxxx/hpif.orig

4. Copy the RCP shell script to the rcp directory /etc/xxxxx. That is:

   cp xxxx.rcp /etc/xxxxx/hpif

5. Edit the interface script and insert the desired Terminal Server name and port number. For example, if the Terminal Server name is 'iceland' and the printer is attached to port 8 (numbering from 1 to 16).

   Then the line:

   rcp $TMP <IOLAN name>:tty<port number>

   becomes:

   rcp $TMP iceland:tty8

   Some Unix systems may require the full pathname of the 'RCP' command. For example, SunOS Unix and may require the line to become:

   /usr/ucb/rcp $TMP iceland:tty8

6. Activate the printer for use. That is:
   lpc start IOLAN8
   lpc enable IOLAN8
7. Set up the Terminal Server port for RCP printing. See the relevant section in the guide or call Technical Support for an example fax.

Setting up RCP printing on AIX

See the our website for latest information.

Tips Hunt groups: There is no hunt group method using RCP.

Chapter 9 Other devices setup

You need to read this chapter if you want to...

You need to read this chapter if you want information on setting up printers and data acquisition type equipment.

This chapter provides information on setting up printers and data acquisition type equipment, including retail point-of-sale equipment.

This chapter includes the following sections;

- **Introduction** on page **111**
- **Reverse Telnet Port Configuration** on page **112**
- **Black Box IOLAND Utility** on page **114**
- **Tips** on page **120**.

Introduction

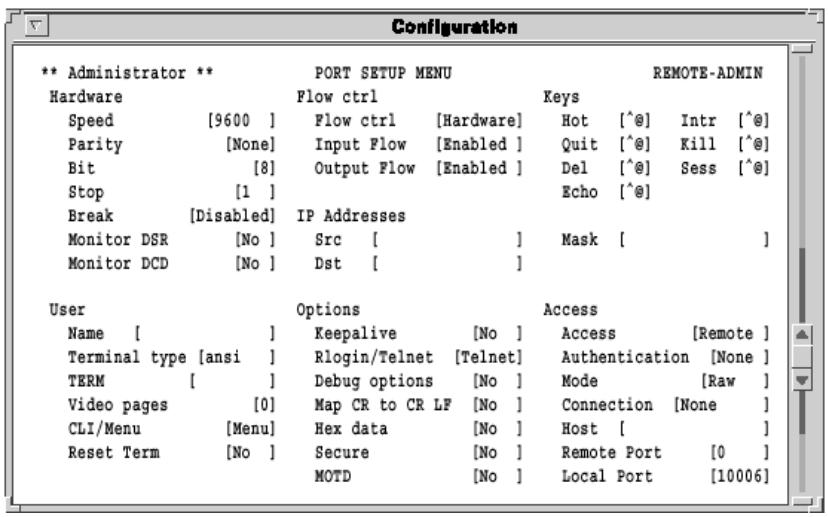
The Terminal Server is a very versatile product and can handle a lot of creative applications. This section deals with setting up printers and data acquisition type equipment, including retail point-of-sale equipment. Many types of RS-232 equipment can be attached including:

- Retail point-of-sale (POS) equipment
- Maintenance ports on network equipment (for monitoring)
- Making terminals with ‘fixed ttys’
- Manufacturing equipment

Your Terminal Server accomplishes this by using a reverse telnet connection. On Unix you utilise the ioland software supplied on the CD. For Windows ® , consult the support section of the web sites for the latest support software for dial-out applications.

Reverse Telnet Port Configuration

This setup is used when you need to access a serial port from the network. For example you might want to collect data from a serial device such as a barcode scanner, POS terminal, etc. Or you can tie a login to a specific Unix tty device (using ioland). For Unix you use the utility ioland. For Windows ® system consult the website.



The following fields are important:

Fields	Description
Keys	Set all your Keys to ^@.
Access	Set this field to Remote. This sets the port of the terminal server to listen for connections coming from the network. There will be an INETD process running on the terminal server that does the listening. You can check on the status of this process by looking at the Netstat screen of the terminal server's Stats menu.
Mode	Set this field to Raw.
Local Port	The INETD process running on the terminal server for this port is listening for TCP/IP connections on TCP port 10006 (for port 6).

If you are already familiar with ioland, all you have to do for the above configuration on Unix is:

ioland -p <server name> 10006 <device name>

This will start the ioland process in permanent mode and create a device in /dev. If you are not familiar with the ioland program, read the following section.

If you are using Windows ® check the web page for the latest information on dial-out connectivity.

Black Box IOLAND Utility

The Terminal Server peripheral daemon provides a client process with a full-duplex and transparent interface to a server port of its choice, via a pseudo-tty device. This presents a tty-like interface to the application in much the same way as a serial port.

The daemon is primarily intended as an interface between the client process and a printer, modem or some data acquisition device. In the case of printers, it is recommended that the LPD protocol is first assessed as a suitable printing solution before the Terminal Server daemon.

By default, the daemon will fork into two processes during the start of a data transfer. The parent process will transfer data from the client to the server while the child process will transfer data from the server to the client. The parent also handles all the control aspects of the client-server link. The child process is normally terminated when the client process closes the slave pseudo-tty unless the -p option is used. In this case, the child is created at startup time and remains.

If the daemon is started without any arguments it will try and open the configuration file /etc/ioland.cf which contains instructions on which daemons to start, for which peripherals, plus any optional arguments.

Alternatively, a single daemon can be started from the shell with various arguments specified.

Mandatory arguments

There are three mandatory arguments the daemon requires to mediate between the client and server port:

Argument	Description
Server	The host name of Terminal Server that has the attached printer or terminal.
Port	The TCP port on which the Terminal Server port is listening for connection requests.
Link	A mnemonic filename in /dev which shall be linked to the slave pseudo-tty selected by the daemon. This should be used as the interface device for client processes since the pseudo-tty may change during the daemon lifetime.

Optional arguments

The other optional arguments modify the behaviour of the daemon in the way it controls connections, and processes data to and from the peripheral. They are defined as follows:

Argument	Description
-T	Enable Telnet protocol processing. This is useful to ensure that the last data block of a print job has reached the Terminal Server before closing the TCP connection. If the end of print jobs are still being lost despite using this option then it is advised to set the stty option 'noflsh' on the slave pseudo-tty if it is supported. This may require the -m or -a options. Alternatively, most line printer spoolers employ a delay before closing the printer port to ensure no pending output is accidentally flushed. It may be possible to increase this delay if the above solutions are not enough. Make sure the port is set to telnet mode in the Port Setup Menu.
-p	The daemon maintains a continuous TCP connection to the Terminal Server port. This is useful for applications that require exclusive and uninterrupted access to a device. Note that no other daemon will be able to access such a port if any daemon is running to that port with this option.
-h	Hangs up the pseudo-tty if the TCP connection is lost. This mimics the situation in which a real serial port loses a signal such as DCD. In the same manner as the serial port, a SIGHUP signal will be sent to all processes that have the slave pseudo-tty as their controlling tty. See the -w option.
-n	Converts all carriage-returns read from the client process to carriage-return and line-feed. This is useful if using ioland for printing and the print job is off the right margin (for example, 'stair stepping').
-m	Push the STREAMS tty modules onto the slave pseudo-tty. This is useful for applications that expect to modify tty parameters as if a hardware device was attached.The modules pushed are the line discipline (normally called ldterm) and the hardware emulation (if supported). This option requires that the pseudo-tty architecture is based on the STREAMS I/O mechanism.The recommended Unix variants for using this option are those based on System V Release 3. Variants based on System V Release 4 should first try the -a option.
-a	Use the autopush facility to push STREAMS modules onto the slave pseudo-tty. This facility is supported on Unix System V Release 4 variants.
-u	Discard all data received from the peripheral. This is useful in cases where the peripheral is sending unwanted data to the host, which is not being read by the client and therefore may cause blockage problems on the pseudo-tty.
-w	Used with the -h and -p options. By default, on a hang-up, the daemon will open a new pseudo-tty before it has reconnected to the Terminal Server port. This option does the opposite and tries to re-establish the TCP connection first.

Argument	Description
-o	Used with the -p option. This option prevents the slave pseudo-tty from closing so as to prevent any flushing of data that may occur. With this option set, the daemon will not close the TCP connection so its use is not advised for modems, as line hang-ups may not be initiated. It is useful for slow printers that may lose data on pseudo-tty close.
-f<file>	Specify a different configuration file. If the pathname is relative, the current working directory will be used.
-F	This option causes ioland to use the same pseudotty each and every time (fixed tty). The syntax for using this option is: ioland -F <other options> <iolan> <master device> <slave device> e.g: ioland -F bronto ptyp3 ttyp3
-k<n>	This option checks if the TCP connection is still alive every n seconds. If the test fails, the child daemon process dies and signals the parent daemon that the connection is lost.
-K	This invokes 'silent keepalives'. Normal keepalives set by the -k flag send ASCII text messages which can go through iolan and ioland and become visible to users and applications. The -K flag prevents this.
-s<desired character transfer rate>	This option causes ioland to 'meter' characters sent to the unit.
-x<n>	Set the daemon debug/diagnostic level to n. On startup, a log file called /etc/ioland.lg is created (if not already there). All daemons on the host will write their debug and diagnostic messages to this file with a timestamp, daemon process id and arguments attached to the actual diagnostic. The debug and diagnostics levels are: 0 Lets the world know we're alive — but nothing else. 1 Reports startup options. 2 Reports connection and disconnection events. 4 Reports numbers of characters being sent/received. 8 Displays data written to the client process. 16 Displays data written to the Terminal Server. 32 Reports telnet negotiations. 64 Displays data read from Terminal Server. 128 Displays data read from the client process. Adding the desired level numbers together can combine these levels. Care should be taken when a high debug level is set because the log file could grow too large.

Argument	Description
-s<string>	Used to transmit breaks to modems. If the daemon reads in the specified string from the client it will send a Telnet ‘Do Break’ command to Terminal Server. The maximum length of the string is 15 characters though, for the sake of efficiency, a minimal length should be used so long as the string is not accidentally duplicated by the real data. This option requires you to also use the -T option.
-c<n>	Network connection timeout option. The daemon will try for n seconds to establish a TCP connection after which time it will abort and discard any pending data. The default is to try forever.

Example daemon configuration file

An example of a daemon configuration file is:

-x3 -T IOLAN1 10011 IOLAN1.11

-x35 -T -a -h -s xxx -c60 IOLAN1 10013 IOLAN1.13

-x39 -p -T -h -a -k60 IOLAN2 10009 IOLAN2.9

Each line represents a daemon to be started with the arguments on that line.

The first is a simple printer configuration, the second is a complex modem configuration while the third is a configuration more suited to a daemon with a terminal attached and a getty running as the client process. Normally, the debug level is set to a minimal level such as three.

Tips

Unix Notes On Unix variants based on System V Release 3, clients that are interactive shell processes may not be able to handle the interrupt, quit and break keys properly. This is a deficiency in the pseudo-tty drivers and not the daemon.

On some System V Release 4 variants, if the daemon writes to a non-existent client, the pseudo-tty may irretrievably hang up. In general, make sure there is always a client process running if there is the possibility of data being received for it.

On some systems such as SunOS, XENIX and AIX a break received from the peripheral is not passed to the client properly. If the client wishes to make the break act like aninterrupt key (for example, when the stty options - ignbrk and brkintr are set) then this can be achieved by setting the Break field on the Terminal Server Port Setup Menu to ‘Brkintr’.

On SunOS, if a getty is the client process running to a terminal then the login prompt may be corrupted on the screen but this goes when the user name is typed in. The UUCP command uucico may not work with ioland on Solaris 2.1 (Intel).

Some systems may not properly propagate the SIGHUP signal associated with the -h option.

Chapter 10 The menu interface

You need to read this chapter if you want to...

You need to read this chapter if you want an overview of the Terminal Server menu interface.

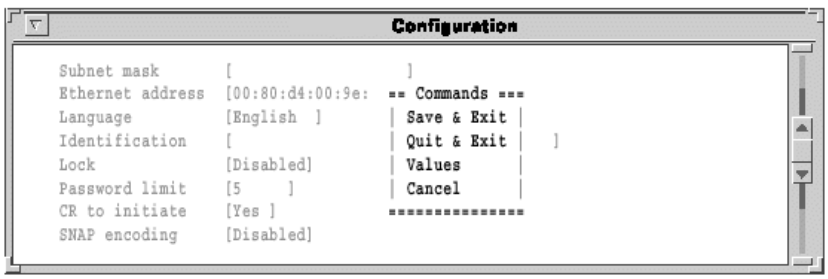
This chapter describes the menu system and the fields within them. All of the menus are covered and referenced in this section.

This chapter includes the following sections;

- **Introduction to menu commands** on page **122**
- **Connections menu** on page **124**
- **Port setup menu** on page **126**
- **Administration menu** on page **135**
- **Access menu** on page **137**
- **Change password options** on page **144**
- **Gateway menu** on page **145**
- **Host Address menu** on page **146**
- **Kill command** on page **146**
- **Lines menu** on page **147**
- **Port menu** on page **150**
- **Quit command** on page **150**
- **Reboot command** on page **150**
- **Server configuration menu** on page **151**
- **Statistics screens** on page **154**
- **Trap function** on page **155**.

Introduction to menu commands

This chapter describes the menu system and the fields within them.You move around the menus with the arrow keys or by using the first letter of the associated command. When you are in an editable menu, the arrow key is used to move around the various fields. Pressing the **Enter** key will usually bring up the following exit menu.



Command Descriptions

Menu option	Description
Save and Exit	All changes to the menu screen are saved and the user is returned to the next higher level screen.
Quit and Exit	The user is returned to the higher level screen and any changes are ignored (that is, nothing is saved).
Values	Certain data fields take only a fixed range of values (for example, bps rates, number of stop bits, etc.). When this command is selected, it displays those values.
Cancel	Cancels the Command Options window and returns to current menu for additional editing.

Pressing Esc cancels the Command Options window (works the same as Cancel). Other than mastering the difference between the arrow key and the Enter key, there are several other special fields and keys.

Toggle fields

Some data fields have a set of acceptable values. An example of this is the bps rate setting. To alter the value displayed in these fields press the space bar. The Values option on the commands pop-up menu can also be used.

Fast keys

A fast key allows the user to jump from one menu to another avoiding the normal path. Most of the commonly used options available from the Connections Menu can be accessed via fast keys. These are listed in the following:

Menu option	Fast key sequence	Description
Telnet	CRTL T	Make a Telnet connection
Rlogin	CRTL R	Make an Rlogin connection
Port	CRTL P	Enter the Port Setup Menu
Admin	CRTL A	Enter the Administration menus
Logout	CRTL D	Log out of the Server
Stats	CRTL X WCRTL T	Enters the statistics screens

Connections menu

This is the top level menu, normally the first thing a user sees when they power up their terminal. The main focus of this screen is the list of connection states, showing which host each of the four sessions is connected to (or if it is FREE).

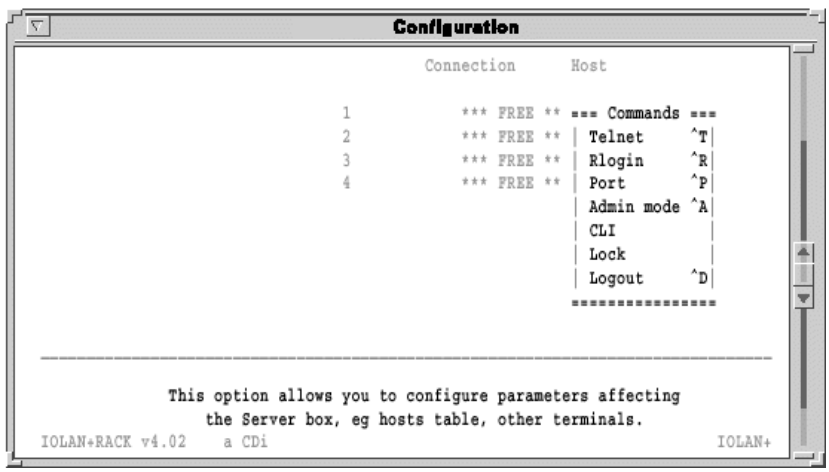


Figure 31: Connections Menu - Commands pop-up menu.

Pressing Enter at any of the four FREE fields presents the Commands pop-up menu. If it was not free, the Telnet and Rlogin fields would have been replaced by Close connection and Resume connection signifying there is a session present.

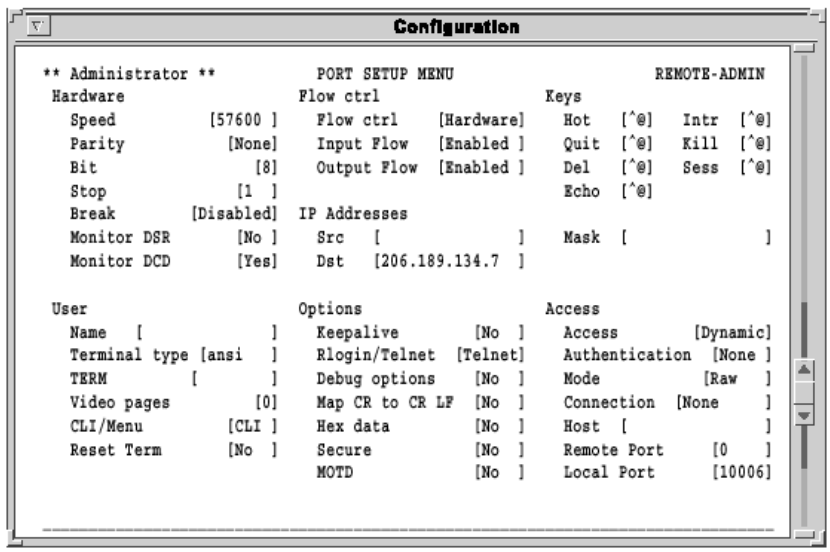
The *** FREE *** message would be replaced by the name or IP address of the connected host.

The following describes the options that can appear in the above menu:

Option	Description
Telnet	This option allows you to make a connection to a specified host on the network using telnet. When this command is selected, another pop-up menu appears, giving you the host table list. In addition, there is a specify host/IP address option you can use for other IP addresses and host names.
Rlogin	This performs the same function as the Telnet open command, but uses the Rlogin protocol. While Telnet is the most commonly used protocol, Rlogin can also be used (especially over WAN connections because Rlogin packets are smaller).
Resume Connection	This option only appears if there is a current connection open. It allows you to carry on working on a host.
Close Connection	This option also appears only if the current connection is open and will close the session on a host machine. It is recommended to logout before closing the connection.
Port	This allows users to change the characteristics of their serial port. See **Port setup menu** on page **126**.
Admin mode	This takes the user into the Administration Menu(s) (also covered in this chapter).
CLI	Selecting this function changes the port back into command line or CLI mode. To get back to the menus use set menu from the CLI prompt.
Lock	This function allows the user to lock the port they are on for security purposes. When this function is selected the user is prompted for a password then asked to verify it again. Once locked a port can only be unlocked by the successful entry of the password. Note: If a user accidentally locks their port the Administrator can use the kill command on the Administration Menu to free the port.
Logout	This function logs the user completely out of the Terminal Server. From the Connections Menu pressing CTRL D also logs the user out of the system.

Port setup menu

This menu allows the user to set up all of the parameters associated with a port. The administrator can alter the set-up of any port on the Terminal Server while a user can only alter the set-up for their own port.



This menu is divided into several separate sections, each of which can be accessed independently by the administrator. To simplify the sequence, these are described separately.

Hardware

The hardware section defines port type and is used for setting up the hardware configuration of the modem, terminal, printer or PC session. This section is always used. The parameters are as follows:

Option	Description
Speed	This field sets the baud rate of the port and can be set to the following values: 50, 75, 110, 150, 300, 600, 1200, 1800, 2400, 4800, 9600, 19200, 38400, 57600, 115200. The default setting is 9600.
Parity	This field sets the parity of the port to even, odd or none. The default parity is None.
Bit	This sets the number of data bits that are used by the port from 5-8. The default is 8.
Stop	This defines how many stop bits the port uses to either 1, 1.5, 2. The default is 1.
Break	This field determines how the Terminal Server reacts to the break key being pressed on the terminal. There are four possible settings: **Disabled** The Terminal Server ignores the break key completely and it is not passed through to the host. This is the default setting. **Local** The Terminal Server deals with the break locally. If the user is in a session the break key has the same effect as a hot key (that is, it returns the user to the Connections Menu.) **Remote** When a break key is pressed the Terminal Server translates this into a telnet break signal which it sends to the host machine. **Brkintr** This mode operates in the same manner as the remote setting except that instead of generating a break signal the Terminal Server generates an interrupt signal and sends it to the host.
Monitor DSR	This field specifies whether the RS-232 signal DSR (data set ready) should be monitored. This is used with modems. Default is No.
Monitor DCD	This field specifies whether the RS-232 signal DCD (data carrier detect) should be monitored.This is used with modems. Default is No.

User

The User section defines various user parameters such as name and terminal type. Most fields are used in this section.

A full description is given below:

Option	Description
Name	This field defines the user name of this port on the Terminal Server. Any string of up to 14 characters can be entered. This name is displayed on the top left hand corner of the menu screens. It is also listed in the statistics screens so that the administrator can see who is using each port. If this field is left blank then a user is prompted for their user name before being given access to the communications server menus. This field is also passed to the host when using telnet or rlogin. Default is blank.
Terminal type	This field defines the type of terminal that is attached to this port. The possible values are undef (undefined), ansi, dumb, vt100, vt320, wyse50, wyse60, tvi925, ibm3151, vt320, falco, hp700. Press the space bar to toggle through these values. If none of these are applicable then the CLI mode can be used. When an rlogin connection is made, the unit passes this terminal type to the host machine. Default is blank.
TERM	This field can contain up to 8 characters. If this field is filled in, the Terminal Server sends this string as the terminal type, instead of the field above. This allows the user to pass through the Terminal Server an unsupported terminal type or addition identity information for security. Default is blank.
Video pages	This field defines how many video pages the terminal in question has. If this value is set greater than zero the Terminal Server uses the video pages on the terminal to allow it to refresh screens between session switching. Not all terminals support video pages (mainly Wyse 60's). Default is 0.
CLI/Menu	This field defines whether the Terminal Server is using the CLI or the menu interface. If the terminal is configured for menu interface but the terminal type is undefined or dumb, then the unit remains in the CLI. Default will be Menu.
Reset Term	This field defines whether the terminal type should be reset when a user logs out. This is a very useful feature when the port is connected to a modem. When a user logs out of Terminal Server it resets the terminal type to dumb, so the next person starts off in CLI mode and is able to set the terminal type correctly. Default is No.

Flow control

This section defines the various flow control options used by the Terminal Server. This section is always used. The parameters are:

Option	Description
Flow Ctrl	This field defines which method of flow control to be used by this port, either XON/XOFF, HARDWARE, BOTH, none or WANG. To use HARDWARE flow control the correct cable must be used (see **Appendix D Cabling**. WANG is a special option designed for WANG terminal flow control applications. The default is to use XON/XOFF.
Input Flow	This field allows you to define if the input flow control is to be used. Default is Enabled.
Output Flow	This field allows you to define if the output flow control is to be used. Default is Enabled.

IP address

This section of the menu deals with remote access and modem sessions only. The parameters are as follows:

Option	Description
Src	This is the source IP address of the port for PPP/SLIP connections. If blank, the Terminal Server IP address is used.
Dst	This is the destination IP address of the PPP/SLIP connections. If blank, the remote host must supply the IP address. If filled in, you designate an assigned IP address to loan the remote host.If the secure field on the Port Menu is No, this can be overridden by the incoming host.
Mask	This is the subnet mask which controls the range of IP addresses accessible from the port (when using remote access).

Options

This section of the menu deals mainly with the telnet options and is the least used. Most of these options default to No.

Option	Description
Keepalive	This option specifies whether the Terminal Server should send keepalive messages to the host machines it is connected to. Default is No.
Rlogin/Telnet	This field specifies which of the two options should be listed first in the Commands menu. Default is telnet.
Debug options	This field defines whether the telnet options processing should be displayed and is used for troubleshooting. Default is No.
Map CR to CR LF	This field defines whether the Terminal Server will add a line feed to every carriage return on data going out to the serial port. Default is No.
Hex data	When this field is set to Yes, the Terminal Server displays all of the data it receives on this port in hex format as well as in ASCII. This is used for troubleshooting. Default is No.
Secure	Specifies the level of security to be applied to the port in question. There are four selectable values. Default is No.
No	Access to the administration mode is enabled from this port. Port will accept IP addresses.
Yes	Access to administration mode is disabled for this port. Port will reject IP addresses.
LAN	Access to administration mode is disabled and dial-in access via PPP/SLIP is disabled. Local network access commands telnet, rlogin and connect are enabled.
WAN	Access to administration is disabled and local network access commands, telnet, rlogin and connect are disabled. Dial-in access via PPP/SLIP is enabled.
MOTD	This yes/no option specifies whether a message of the day is to be displayed to the user before logging on to the port. The actual text of the message is a file on the boot host (see **Server configuration menu** on page **151**).

Keys

This section defines the various accelerator keys that the Terminal Server responds to. This section is optionally used. The parameters are as follows:

Option	Description
Hot	This is the key used to escape from a host connection back to the Terminal Server Connection Menu. For instance, if you are in a login shell on a host machine, pressing the hot-key takes you back to the Terminal Server. The default is ^].
Intr	This is a user-definable interrupt key. When selected the Terminal Server generates a telnet 'interrupt process' signal to the remote host. The default is ^C.
Quit	This field defines the character that generates a telnet BREAK across the network. Default is ^@.
Del	This field defines the character that generates a telnet erase character signal across the network. In addition, this key can be used to 'reprogram' the interpretation of the <left-arrow> key when operating in the menu mode. If the users terminal generates the same key sequence for <Left-Arrow> and <Backspace>, then setting this key to Ctrl-H (^H), causes the <Left-arrow> and <Backspace> keys to be treated as 'delete the last character typed in'. Default is ^@.
Kill	This field defines the character that generates a telnet erase line signal across the network. Default is ^U.
Sess	This key allows users to switch directly from one session to another without going back through the server menus. This key should be followed immediately by the session number the user wishes to go to. For example, if this key is set to Ctrl-F and you want to switch to session 2, press Ctrl-F2. The default value is ^@.
Echo	If this key is given a value then any active telnet session on that port can toggle between local and remote character echoing done by the Terminal Server or by the remote host. Default is ^@.

Note

Each of the keys can be set as a single character, or as a control character. To set the key as a control character the symbol '^' should be used followed by the relevant key. Alphabetic characters should be specified in upper case. To disable a particular key the user should enter ^@ in the field.

Access

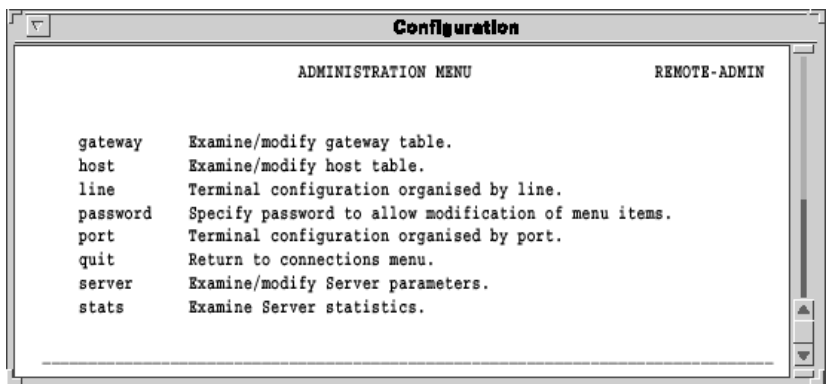
This section controls the type of the connection made from this port. This is the most important section in defining a port. The parameters are as follows:

Option	Description
Access	This field defines the type of service that is operating on this port. Default is Local.
Local	This is the normal setting for terminals/PCs.
Remote	This setting indTerminal Server should be listening on the ethernet for connections from a remote host. The TCP port for the communications server to listen on, must be entered in the Local Port field. This setting should be used for printers, dial-out modems and reverse telnet connections.
Dynamic	This setting should be used for dial-in/dial-out modems. This setting is a combination of the local and remote settings. The communications server listens both on the serial port for incoming characters and on the network for incoming connections. When it gets either, it behaves as the appropriate type of connection until that session is terminated, whereupon it goes back to listening again.
UDP	This setting indicates the Terminal Server should be listening on the ethernet for connections from a remote host. The UDP port for the communications server to listen on, must be entered in the Local Port field. When using UDP access, the Host field and the Remote Port field can be left blank and can be determine from the first datagram recieved on the Local Port.
SLIP	This will set the port into SLIP mode.
PPP	This setting puts the port into a dedicated PPP line.
Listen	This setting is similar to Remote, however, DTR/RTS will only be raised once a network connection is establish.
None	Sets port to disabled.
CSLIP	This setting puts the port into dedicated CSLIP status.
Vmodem	This setting causes the Terminal Server port to behave as if it were a modem to the attached device. See the **Chapter 7 Vmodem (Virtual modem)** for details.

Option	Description
Authentication	This field defines how a user logs in. Default is none. None This sets authentication off. Local This forces the incoming user to enter the Terminal Server login authentication password (same password for all ports). Host This is full authentication requiring a user ID and password that will be checked against a designated authentication host. Both This provides two levels of security with Local authentication first, then Host.
Mode	This field defines whether the connection is raw or telnet. A raw connection is a straight TCP connection. Setting the mode to telnet causes it to do the telnet negotiations with a network connection. This should be set to raw for RCP and LPD printing & modem connections, and be set to telnet for reverse telnet connections.
Connection	This field defines whether the user has access to multiple connections or only a single connection, and the level of control the user has over these connections.
None	Terminal Server does not try to initiate any connections. The user has full control and, access to all 4 sessions. This is the default.
Preferred	Terminal Server makes an immediate connection to the indicated host machine and port number. The Host, Remote and Mode fields must be filled in. Although the user is connected to a designated host, the user can hot key ^] back from this connection to the unit. This allows a user to configure the system so that they always log into one machine, but still have the option of connecting to others.
Dedicated	Terminal Server makes an immediate connection to the indicated host and port number. The user is limited to only a single connection to the indicated host, and can not hot key back to the Terminal Server menus. The Host, Remote and Mode fields must be set properly.
Initiated	This setting is similar to the Dedicated connection, but requires the user to enter the return key before initiating a connection. It is widely used for terminal/PC connections.
Host	This field defines the remote host to be connected to. Either a host name or an IP address may be used. If a name is entered it must be in the host table. Default is blank.
Remote Port	This field defines the remote TCP or UDP port number for the Terminal Server to connect to. Use port number 23 for telnet and 513 for rlogin. Default is 0.
Local Port	This field defines the local TCP or UDP port number for the Terminal Server to listen on. The port default to 10000 plus the number of the port.

Administration menu

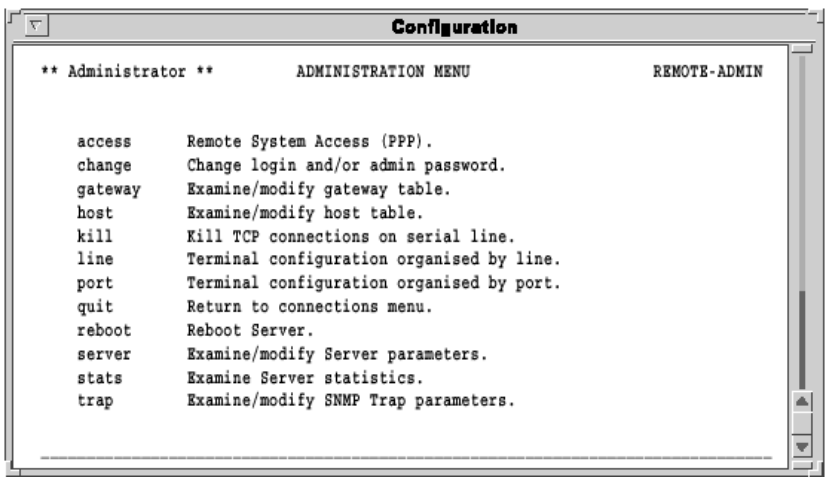
The Administration Menu allows the user access to the main configuration functions. All of the options can be accessed by a normal user (unless the secure field is set to Yes). None of the configuration details may be altered unless the user has entered the administrator's password.



The parameters are as follows:

Option	Description
gateway	Selecting this field allows the user to view the Gateway Menu used for routing.
host	Selecting this field allows the user to view the Host Address Menu used for local naming.
line	Selecting this field takes the user to the Lines pop-up menu used for viewing port configurations.
password	Selecting this field allows the user to enter the administrator's level where changes can be made. Default password is iolan.
port	Selecting this field allows the user to view the Port Setup Menu as previously described. The user is prompted for the port number to be configured.
quit	Selecting this field takes the user back into the Connections Menu.
server	Selecting this field allows the user to view the Terminal Server Configuration Menu.
stats	Selecting this field allows the user to view the Terminal Server Statistics screens.

Once the user has entered administration mode the display changes slightly to indicate this.

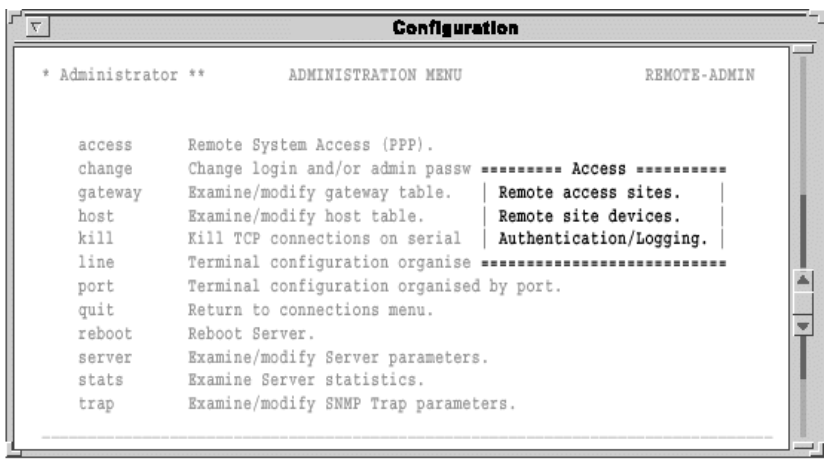


This allows the user access to some extra features as follows:

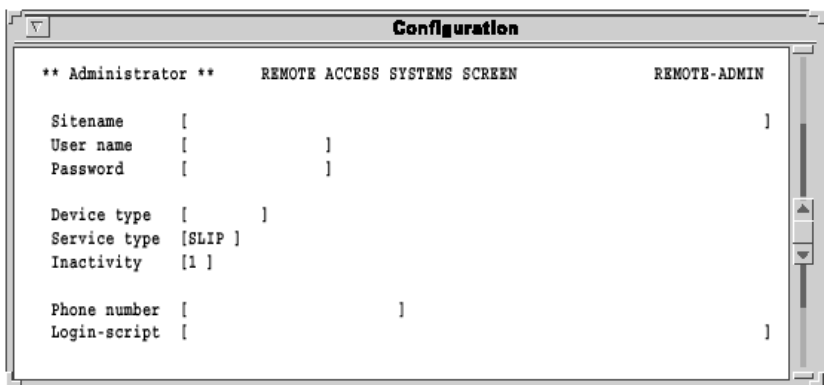
Option	Description
access	Selecting this option takes the user into the remote access section of Terminal Server bringing up a menu for designating remote sites, devices and authentication/logging parameters.
change	Selecting this field takes the user into the Password pop-up menu. The user has the option of altering the admin, login or logger passwords.
kill	Selecting this field allows the administrator to reset any serial port. The administrator is prompted to enter the port number and press the **Enter** key.
reboot	Selecting this field allows the user to reboot the Terminal Server.
trap	Selecting this field will take the user into the SNMP trap function menu.

Access menu

The Access section deals with remote access sites, devices and the authentication and logging parameters. The initial pop-up window is as follows:



This first brings up a pop up menu with 16 possible UNUSED ENTRYs. These will represent the available dial-out sites for Terminal Server. Selecting any of these will bring up the following menu:

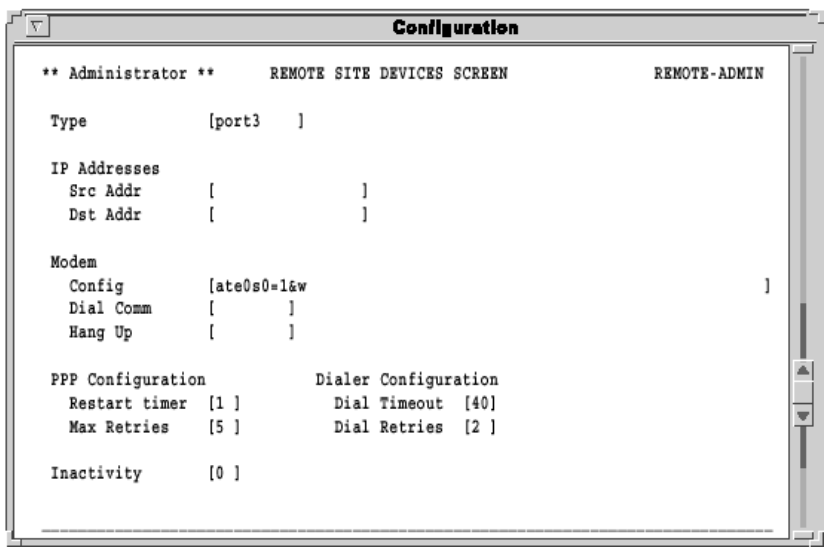


The parameters are as follows:

Parameter	Description
Sitename	This is the IP name or IP address of the remote site the Terminal Server will be calling.
User name	This is the user name required by the remote system for logging in. You may use the \u in your login script in lieu of the full name.
Password	This is the above user name's password as required by the remote system. You may use the \p in your login script in lieu of the full password.
Device type	This is the name of the modem device as defined in the Remote Site Devices screen. You may have several ports setup with the same device type, and the dialer daemon will use the first available. If a device for dialling out is not available, Terminal Server will return an ICMP 'host unreachable' message (ICMP type 3 code 1).
Service type	This specifies which protocol will be used when the link is established to the remote site. Choices are SLIP, CSLIP or PPP.
Inactivity	This is the period of inactivity on the SLIP/PPP link before the port will drop the call automatically. Setting this field to 0 turns the timeout feature off.

Parameter	Description
Phone number	This is the phone number of the remote system. The '\' may be used as a delay. For example, a phone system that requires a 9 followed by a four-second delay before getting an outside line would require an entry like 9\4-2145551234.
Login-script	This is the chat script that will be used to login to the remote system. It takes the form of the usual Send/Expect chat script you may already be familiar with. If no script is defined, this step is skipped (for example, hardwired connections).

This first brings up a pop-up menu with 16 possible UNUSED ENTRYs each corresponding to a port.



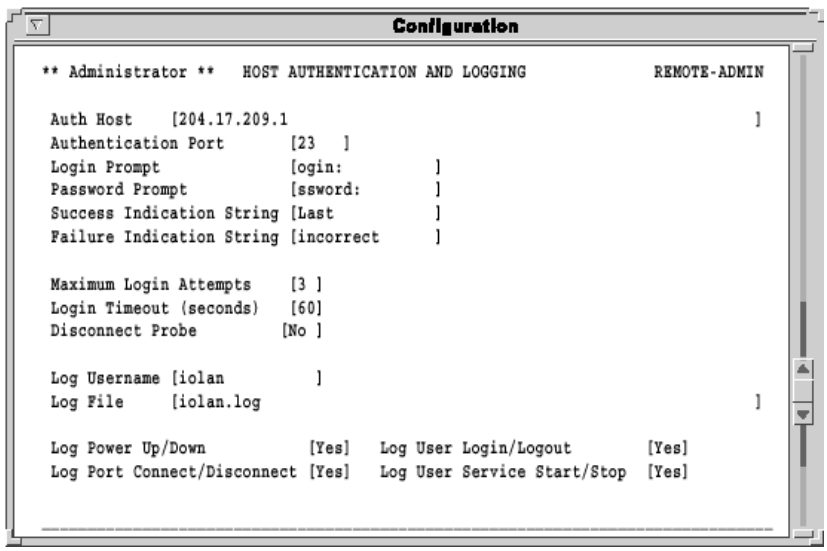
The parameters are as follows:

Parameter	Description
Type	This is the name of the modem assigned to a specific port. It is referenced from the Remote Access Systems Screen in the Device type field.
Scr Addr	This is the source IP address of the port for remote access/modem configuration. If blank, the Terminal Server IP address is used.
Dst Addr	This is the destination IP address of the port for remote access/ modem configuration. If blank, the remote host must supply the IP address. If filled in, you designate an assigned IP address to loan the remote host. If the secure field on the Port Menu is No, this can be overridden by the incoming host.
Config	This is the modem's setup string. There are a few examples at the end of this document. Note: Leave this field blank for directly connected devices.
Dial Comm	This is the modem's dial command.
Hang Up	This is the modem's hang up command.

Parameter	Description
Restart timer	Amount of time in seconds before the Terminal Server retransmits PPP options.
Max Retries	Number of option retries before dropping the line.
Dial timeout	Number of seconds to wait for the modem to establish link and respond.
Dial retries	Number of times to attempt a connection to the remote site before giving up.
Inactivity	Number of minutes of inactivity before a PPP/ SLIP connection is broken.

Authentication/Logging

This section outlines the authentication and logging parameters of the Terminal Server.



The parameters are as follows:

Parameter	Description
Auth Host	The IP name or address of the authentication host to validate incoming users.
Authentication Port	The TCP port number of the authentication host, usually 23 (telnet) or 513 (Rlogin). A proprietary network number may be chosen to provide a personal user validation scheme. Default is 23 (telnet).
Login Prompt	The user authentication prompt expected from the host by the Terminal Server. Default is ogin:
Password Prompt	The password prompt expected from the host by the Terminal Server during the authentication connection.Default is ssword:
Success Indication String	The string returned by the authentication host on successfully logging in. Default is Last
Failure Indication String	The string returned by the authentication host on a failed login attempt. Default is ogin incorrect.

Parameter	Description
Maximum Login Attempts	The maximum number of login attempts a user is allowed before the line is reset. For modem users the control line DTR is toggled, the port is disabled for 3 seconds. Default is 3.
Login Timeout	This time defines the maximum time in seconds for the user to enter authentication information, once login time-out is exceeded the line is reset.Default is 0.
Disconnect Probe	An option to keep the per port authentication connection up during the clients' session. Default is Yes. This allows a user connect time to be measured by a simple 'do nothing' telnet session.
Log Username	The logger's user name for gaining access to the log file on the host. Log File The pathname of the activity log file.
Log Power Up/Down	Logs port connection status to the log file (for example, for Dial-in users). Default is No.
Log User Login/Logout	Logs a message to inform the host when the Terminal Server is powered up and when rebooted from software. This logs an 'I am alive' message every five minutes. Default is No.
Log Port Connect/ Disconnect	Record users logging into authentication host on the log file. Also records failed login attempts. Default is No.
Log User Service Start/ Stop	Logs starts and stops of PPP or SLIP. Default is No.

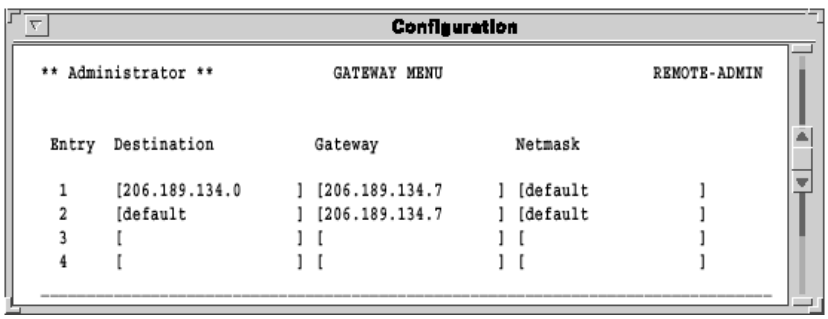
Change password options

This option allows the administrator to change the admin, login or logger passwords. It is recommended to change the password from the default iolan. The following selections can be called from the Administration Menu, **password** option:

Password option	Description
Admin Password	The user is required to enter the new administrator's password twice.
Login Password	The user is required to enter the Terminal Server login password twice.
Logger Password	This field allows the user to change the log user password.

Gateway menu

The Gateway Menu allows the Terminal Server to make use of a gateway (I P router) on the network. This allows flexible internet working.

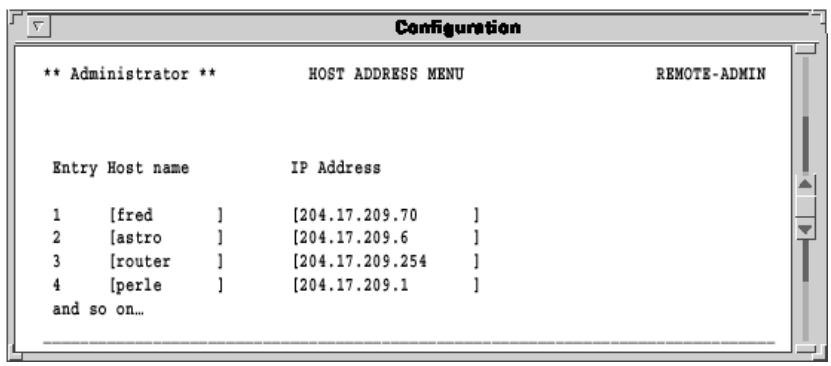


The parameters are as follows:

Parameter	Description
Destination	This field specifies either the destination network or host address.
Gateway	This field defines the gateway (IP router) host address. The gateway host must be attached to the same network as the Terminal Server.
Netmask	This field allows the administrator to define a mask that the Terminal Server will use to mask out packets from other networks using the same Ethernet.The valid Netmask fields are: **class a** Only class a addresses are allowed across the gateway. **class b** Only class b addresses are allowed across the gateway. **class c** Only class c addresses are allowed across the gateway.
host	The Destination field is a host IP address and only packets for that host are allowed across the gateway.
default	Any IP address allowed across the gateway
<dot notation value>	Only addresses fitting the numerical mask are allowed across the gateway.

Host Address menu

Your Terminal Server uses the information entered on the Host Address Menu to form an internal host table. The user can then use the host name in any of the Terminal Server functions or menus.



The parameters are as follows:

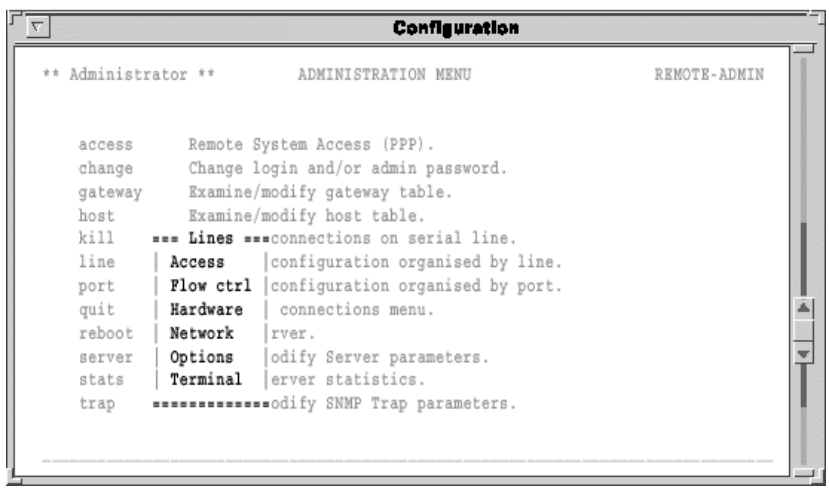
Parameter	Description
Host name	This field specifies local name you want to give a particular host on the network.
IP Address	This field defines the IP address of the host designated above.

Kill command

The kill command resets the port but keeps the previously defined configuration. This is used when you change certain parameters or for when ports get stuck.

Lines menu

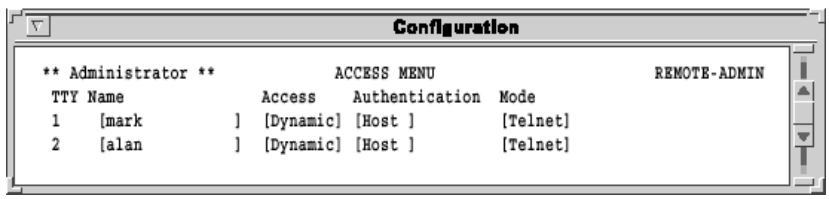
This option allows the administrator to configure all of the parameters for any of the ports. The parameters accessible are exactly the same as those in the Port Setup Menu, but from these menus you can configure a set of parameters for all of the ports. Selecting this option brings up the Lines pop-up menu as shown below.



Each of the options displayed in the pop-up menu brings up another menu. These are detailed in the following sections.

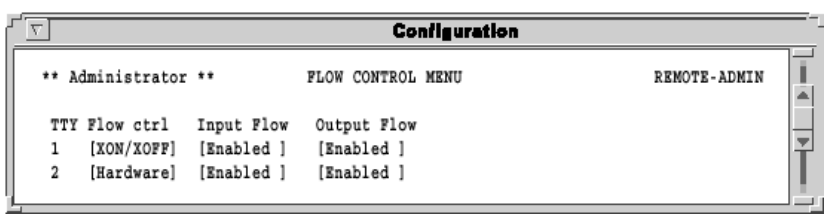
Access

The Access section shows and allows changes to the name, access, authentication and mode fields. These fields are described in **Port setup menu** on page **126**.



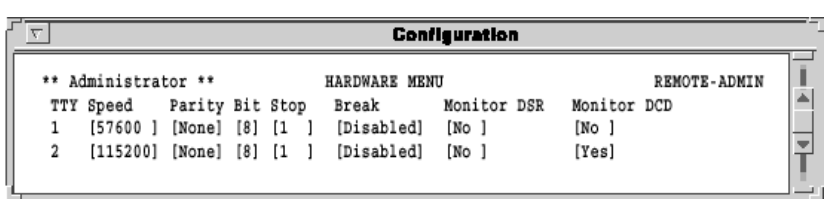
Flow control

The Flow Control section shows and allows changes to the flow control fields as described in **Port setup menu** on page **126**.



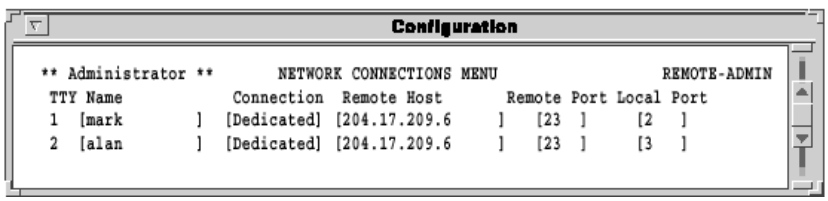
Hardware

The Hardware section shows and allows changes to the hardware control fields as described in **Port setup menu** on page **126**.



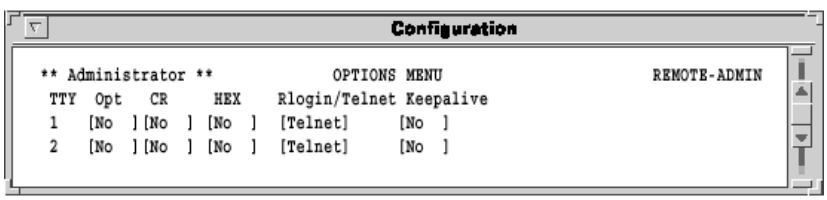
Network connections

The Network Connections section shows and allows changes to some of the Access fields as described in **Port setup menu** on page **126**.



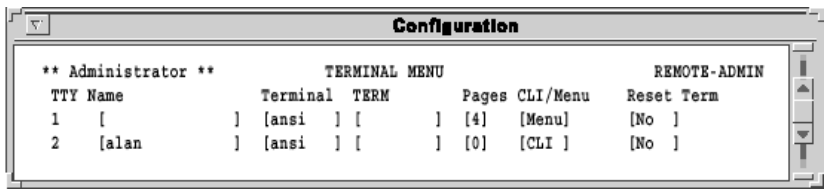
Options

The Options section shows and allows changes to the Options fields as described in **Port setup menu** on page **126**.



Terminal

The Terminal section shows and allows changes to some of the User fields as described in **Port setup menu** on page **126**.



Port menu

This section is covered under **Port setup menu** on page **126** of this chapter.

Quit command

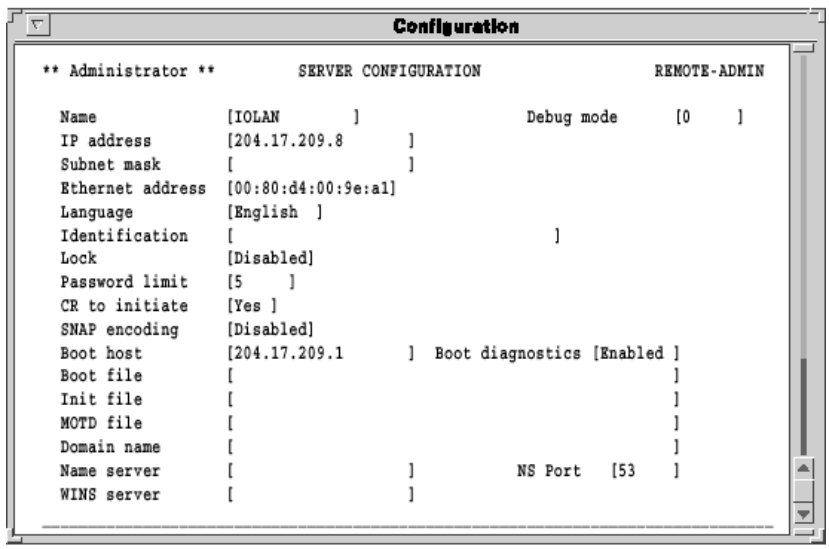
This command simply quits out of the password level up to the view-only administration level (the ESC key works as well.)

Reboot command

This option initiates a reboot of the unit and should only be used for changing the IP address or netmask options. It also can be used for troubleshooting. The user will be given a last option to quit before rebooting.

Server configuration menu

This menu allows the user to define all of the main Terminal Server system parameters.



The menu as displayed can be divided into four logical sections: identification fields, general admin, downloading and domain naming.

Identification fields

Field	Description
Name	This field determines the name of the Terminal Server and is displayed in the bottom right hand corner ofthe menus.
IP address	This field holds the IP address of the Terminal Server. If the IP address of the unit is altered then the unit must be rebooted to permanently save changes.
Subnet mask	This field allows the administrator to define a mask that the unit uses to mask out packets from other networks using the same ethernet.
Ethernet address	This field defines the globally unique ethernet address of the Terminal Server. This address can not be altered and matches the address provided on the physical back of the unit. In the unlikely event of this field being corrupted please contact your supplier.
Ethernet interface	This field defines which Ethernet media will be used. The LAN connectors are autosensing but you can change this to a specific interface.

Field	Description
Language	This field determines the language that the Terminal Server is using such as English, French, German, etc.
Identification	This field allows the administrator to enter an identification string into the unit and is displayed at the bottom of the menus.
Debug mode	This field is for Technical Support use only.

General administration

Field	Description
Lock	This field determines whether the Lock feature is available to all users. If this field is set to disabled then nobody can use the Lock feature.
Password limit	This field defines the number of attempts a user is allowed to enter the correct password for a port. If the user exceeds this limit the Terminal Server disables the port for 5 minutes. The Administrator can restart the port, bypassing the timeout, by issuing a kill on that port.
CR to initiate	This is the 'carriage return to initiate' field which designates that when terminals are setup for initiated connections, the user must hit **Enter** to establish a connection. Otherwise, any input will startup the connection (even noise on the cable).
SNAP encoding	This is an alternate Ethernet encoding (SubNet Access Protocol).

Downloading

Field	Description
Boot host	This field should only be filled in if the Administrator wishes to download a new firmware version. It contains the host name or IP address of the host machine that has the Terminal Server download image on it.
Boot file	This field contains the full path and file name of the Terminal Server download image (including path name). Boot host required.
Boot diagnostics	This port (if enabled) allows the TFTP download state to be displayed on port 1 and is used for troubleshooting. Boot host required.

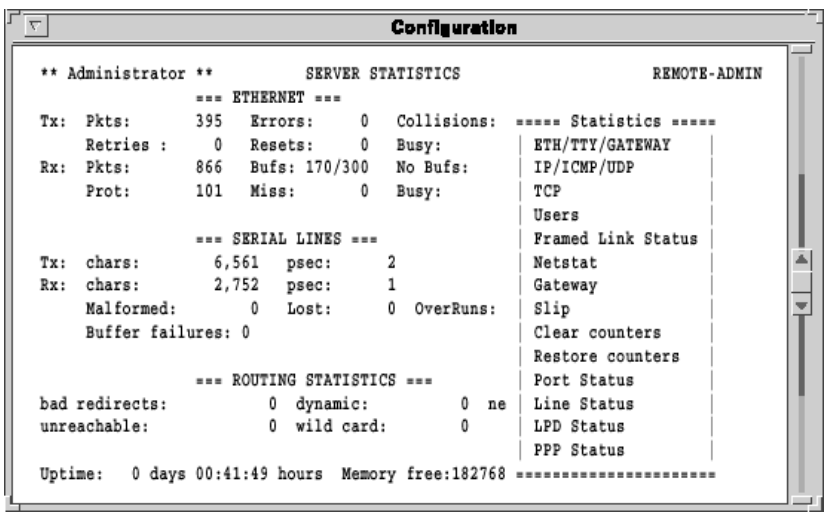
Field	Description
Init file	This field contains the file name of the Terminal Server configuration image. If this field is present, the unit reads its configuration from this file whenever it is rebooted. Boot host required.
MOTD file	This field should be filled in with the pathname of a file on the boot host containing the message of the day text to be displayed on any selected ports. A filename or relative pathname entry assumes the top level directory is /tftpboot. Boot host required.

Domain naming

Field	Description
Domain name	This field should contain the domain name for the name server.
Name server	This field should contain the host name or the IP address of the host machine being used as a Domain Name Server.
WINS server	This defines the Windows ® name server on the network and allows dial-in users full access to the network.
NS Port	This field contains the TCP port number of the Name Server service on the host machine. The default value is 53.

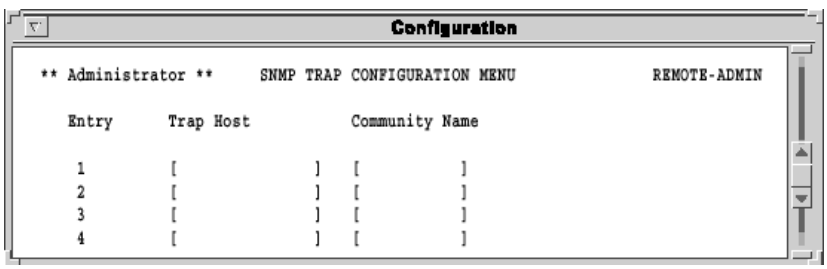
Statistics screens

The statistics screens are used for troubleshooting only. This main screen shows the sub-menus that can be addressed. For more information on the statistics menu, see **Appendix B Troubleshooting**).



Trap function

This is the SNMP trap setup which allows SNMP trap messages to be sent to up to four hosts. Trap messages are sent at system startup and detection of security violations.



Field	Description
Trap Host	This field is the IP address of the trap host.
Community Name	This is the community (password) of trap host.

Appendix A Command Line Interface

You need to read this chapter if you want to...

You need to read this appendix if you want an overview the Terminal Server command Line Interface.

This appendix describes the Terminal Server Command Line Interface including information on using the CLI as well as listing the command syntax.

This chapter includes the following sections;

- **Introduction** on page **157**
- **Using the CLI** on page **158**
- **System administration** on page **159**
- **Basic configuration** on page **160**
- **Command descriptions** on page **161**

Introduction

This chapter outlines the use of the command line interface as opposed to the menu system. The Terminal Server supports the use of menus for a number of terminal types. It also supports a command line interface (CLI) for use on other terminal types and Telnet/Rlogin sessions.

If possible the menu interface should be used as it is far simpler to use. However, the CLI does offer the same level of functionality.

Using the CLI

The Terminal Server command line consists of a prompt as shown below.

local>

The Terminal Server accepts commands in both lower and upper case, and shortened versions of commands can be used as long as they only have an unambiguous meaning. For example 'tel' could be used in place of 'telnet'.

Your Terminal Server offers an extensive help facility. To enter the help function type,

local> help

The Terminal Server responds as follows,

```
Help is available for the following commands:

CONNECT CLEAR   COPY   DISCONNECT
EXIT    GATEWAY HELP   HOST
KILL    LOCK    LOGOUT RESUME
REBOOT  RLOGIN  SAVE   SET
SHOW    SU      TELNET TEST
ARP     PROV    DIAL   FACRESET
Topic?
```

The user may now type in any of the indicated topics and press the Enter key. This gives more information on the indicated subject in the form of syntax and synopsis. In some cases, a further choice for more information (stating 'additional help is available for' and another list).

System administration

To gain access to all of the configuration functions of the Terminal Server a user must log in as the administrator. To do this type:

```
local> su
Password>
```

The user must enter the administration password. The default password is iolan (lower case), but it is suggested that this be changed to prevent unauthorised access. If you are logged in as the administrator then the prompt is as follows:

```
ADMIN:local>
```

Once logged in the administrator can alter the parameters on another port, reboot the Terminal Server or change any of the system parameters.

Basic configuration

To setup your communications via the command use the following instructions:

1. Enter administrative mode, password level:

   local> su
   Password>

2. Enter set server. This will lead you to:

```
ADMIN:local> set server
Type '?' at prompt to see list of valid options;
<Esc> to abort changes.
Name : ronald
Debug mode : 0
IP address : 204.17.209.18
Subnet mask : 255.255.255.0
```

   and so on…

3. Enter reboot .

```
ADMIN:local> reboot
```

Command descriptions

There are a large number of commands available for the Terminal Server, these are detailed below:

arp

Syntax: arp [flush]

Description: This command by itself will show the IOLANs arp table (IP address, Ethernet address, flags). In the admin mode, using arp flush will clear all the entries in the arp table. This is used to clear arp entries when you want to change the Ethernet address of a device.

clear

Syntax: clear

Description: This command clears the screen.

connect

Syntax: connect [host] [port]

Description: This makes a telnet or rlogin connection to the indicated host or IP address. If the user omits the host/IP address then the Terminal Server asks for it as shown below. The command will use telnet or rlogin depending on what is set in the Options section of the Port Menu.

Example:

```
local> connect
Host/IP Address> microart
TCP Port> 23
```

> Note
>
> If the user presses the return at the port prompt, the unit defaults to port 23 which is the standard telnet port (or 513, the standard rlogin port). This option is not available when using remote administration or if the port secure mode is WAN.

copy

Syntax: copy <source port> <destination> [destination]…

Description: This command copies one port setup to another allowing easy setup if the ports are the same configuration. Administrative level is required to change. Note that multiple destination ports can be specified separated by spaces.

dial

Syntax: dial

Description: This command shows the status of the dial-out interface and would be used for monitoring dial-out connections.

disconnect

Syntax: disconnect <session-number>

Description: This command allows a user to disconnect (close) one or all of their existing TCP connections.

exit

Syntax: exit

Description: This function causes the user to exit the Terminal Server, closing down any sessions and resetting the port. Some configuration parameters only come into effect after the user has exited and re-entered Terminal Server (e.g. the name field).

facreset

Syntax: facreset

Description: This function will reset all parameters back to factory defaults. This option requires confirmation.

gateway

Syntax: gateway <[add dest gate net][delete dest]>

Description: This function allows the administrator to alter the gateway routing table. New gateways can be defined by using the add function, and gateways removed using the delete function. When adding, admin level required to change.

help

Syntax: help

Description: This function provides syntax descriptions and partial descriptions of the available commands.

host

Syntax: host <[add name address][delete name]>

Description: This function allows the administrator to add and remove names from the host table. The name can be anything up to 18 characters long, and the address field is the IP address of that host. There can be a maximum of 10 entries in the host table. Admin level required to change.

kill

Syntax: kill <port number>

Description: This function allows the user to reset their own port, or the administrator to kill any other ports. When kill is issued any existing sessions are terminated and the port set back to its starting state. Admin level required.

lock

Syntax: lock

Description: This function allows the user to lock his terminal using a specific password. The Terminal Server prompts the user for a password and a confirmation. This function can not be used unless the Lock enable flag is set (via set port command).

logout

Syntax: logout

Description: This function causes the user to exit Terminal Server. The unit closes down any sessions and resets the port. Same as exit.

prov

Syntax: prov

Description: This function displays the network status of each IP provider and is used for troubleshooting.

reboot

Syntax: reboot

Description: This function reboots the terminal server. Admin level is required.

resume

Syntax: resume <session number>

Description: This allows user to resume an established connection if there are multiple sessions going.

rlogin

Syntax: rlogin [host] [port]

Description: This function allows the user to make an rlogin connection to the specified host machine. If the port number is not specified then it defaults to 513.

save

Syntax: save config

Description: This function allows the user to save the Terminal Server configuration to a specified host machine and file. The configuration is saved to the specified Boot Host and put into the file name described in the Init File parameter (see **set server** on page **166**). The Terminal Server uses the TFTP protocol to save and load the file.

Because of a restriction in most TFTP implementations the file must exist before it can be written. Admin level is required.

Example: To create the file under Unix type:

```
touch filename
chmod 666 filename
```

set

Syntax: set <parameter> [value], etc.

Description: The set command allows the administrator to configure any of the Terminal Server parameters. It also allows the user to alter their own set-ups and change terminal type. Admin level is required on most functions.

set admin

Syntax: set admin

Description: This function allows the user to become the administrator or admin level. The command su can also be used.

set menu

Syntax: set menu

Description: This function sets the user's port into menu mode, assuming that the term type has been set.

set modem

Syntax: set modem

Description: This function transmits a series of modem initialisation commands to the attached modems. A sequence of port numbers from 1 upward can be given or all to indicate all serial ports. The modem commands are taken from the Modem Config field of the Remote site devices menu.

set term

Syntax: set term

Description: This function allows a user to alter their terminal type. If the term field is left blank the Terminal Server displays a list of all the currently supported terminals (ansi, dumb, vt100, wyse50, wyse60, tvi925, ibm3151, vt320, falco, hp700).

set port

Syntax: set port

Description: This function allows a user to set the parameters for their port, or the administrator to set the parameters for any port. The user will be prompted for each parameter in this section (e.g: speed, parity, etc.).

set port [number]

This allows the administrator to set all of the port parameters for the indicated port.The user will be prompted for each parameter in this section.

set port [number] [access, flow, hardware, options, tcp, user]

This allows the administrator to set all of the port parameters for the indicated port in the indicated section. E.g. set port 1 access would prompt through the access section of the port screen 1. If no number is given, it gives your current port parameters.

set server

This function allows the administrator to alter the Terminal Server set-up including initial IP address and name.

set slip [IP address]

This function causes the port to go into SLIP mode provided secure is not set to LAN. You can specify an IP address to used by the remote host.

set ppp [IP address]

This function causes the port to go into PPP mode provided secure is not set to LAN. You can specify an IP address to used by the remote host.

set password [admin] or [login]

This function allows you to change the admin or login passwords of the Terminal Server.

> Note
>
> The remote access functions of your Terminal Server unit are not configurable from CLI (for example, the Access section of the Administrative Menu).

show

Syntax: show <parameter>

Description: This function allows the user to see most of the Terminal Server configuration parameters, but not change them. The set command is used to configure the ports. The show command works with gateway, hosts, netstat, server, sessions, slip, extra, users, version.

show ports

The show ports command requires the port number.

Example: show port 1 would show all the port settings for port 1.

show lines

The show lines command requires which fields you wish to view on all ports (access, flow, hardware, options, tcp, user).

Example: show lines access would show the access settings of the port menu.

show statistics

The show statistics command is used to display any of the Terminal Server statistics for troubleshooting only (tcp, ip, udp, icmp, tty, eth, gateway).

Example: show statistics tcp would show the TCP parameters screen. You can add a delay option which updates the screen every n seconds such as: show stats tcp 3 (use ESC to quit).

su

Syntax: su

Description: This function allows the user to become the administrator. When this command is entered the Terminal Server prompts the user for the admin password which is iolan by default (please change for better security).

telnet

Syntax: telnet [host] [port]

Description: This function allows the user to make a telnet connection to the specified host and port number. If the user does not specify the port your Terminal Server defaults to port 23 which is the defined Unix telnet port. If the host name is not defined then the unit prompts the user for the host and port.

test

Syntax: test [port port_number] [count <n none>]

Description: This function causes your Terminal Server to run a simple output test on the port. The Terminal Server outputs a continuous stream of data in a preset pattern.

To stop the test press any key.

Appendix B 48V DC Rack Terminal Server

You need to read this chapter if you want to...

You need to read this appendix if you want information on the Rack Terminal Server for 48V DC supply.

This appendix describes the 48V DC version of Rack Terminal Server which has been designed specifically to operate on a telecoms compatible 48V DC supply. Please read these instructions carefully before commencing installation.

This chapter includes the following sections;

- **Introduction** on page **170**
- **Installing the Rack Terminal Server 48V DC** on page **171**
- **Electrical Safety Guidelines** on page **173**
- **Connecting up your Rack Terminal Server** on page **173**
- **Disconnecting your Rack Terminal Server** on page **173**.

Introduction

This version of the Rack Terminal Server has been designed specifically to operate on a telecoms compatible 48V DC supply. Please read these instructions carefully before commencing installation.

The 48-60VDC supply range marked on the equipment is the nominal voltage associated with the battery circuit of a centralised DC supply system. Higher voltages are only to be associated with “float” voltages for the charging function.

Installing the Rack Terminal Server 48V DC

Installation

The Rack Terminal Server 48V DC is designed for professional installation in a restricted access area. The installation should comply with current local or national standards applicable to the territory where the Rack Terminal Server is installed.

Warning

The Rack Terminal Server 48V DC shall be installed in a closed rack system with a power distribution unit. A listed branch circuit over-current protective devices rated at 3 amps DC shall be provided either in the power distribution unit or between the power distribution unit and the Rack Terminal Server.

Electrical Supply Details

The Rack Terminal Server is supplied with an Input Power cable (802-0061). This should be connected to your 48V DC supply system which should have adequate over-current protection within the closed rack system and comply with current local or national standards applicable to the territory.

Warning

This equipment must be earthed for safety and to ensure ESD protection for correct operation and protection of the internal circuitry.

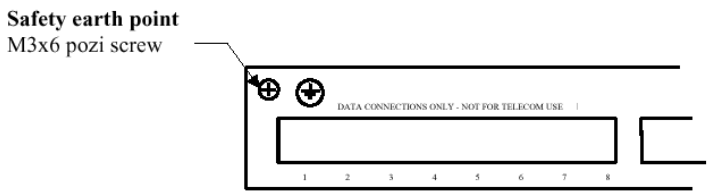
Connect the input power cable to your over-current protected power distribution unit as follows:

Red Positive

Black Negative

White Ground/earth

Safety Earth



Warning

This apparatus must be earthed.

A safety earth point is provided on the rear on the unit. A suitable earth cable of at least 20awg should be attached using the M3 pozi head screw and shakeproof washer to the safety earth point on the rear of the unit.

Fusing

CAUTION: for continued protection against risk of fire, replace only with same type of and rating of fuse.

The Rack Terminal Server 48V is fitted with a 1 Amp time delay DC rated fuse (6.3 x 32 mm). In the event of a fuse failure, it must be replaced with an equivalent type.

Recommended fitment is Bussmann MDA1.

Electrical Safety Guidelines

Warning

Electrical current from power, telephone and communications cables may be hazardous. Connect and disconnect cables in the order detailed below when installing, moving or opening the covers of this product or attached devices.

During periods of lightening activity, do not connect or disconnect any cables or perform installation, maintenance or configuration.

Connecting up your Rack Terminal Server

Making connections to your Rack Terminal Server should be performed in the following sequence:

1. Switch off the power source.
2. Connect attached devices
3. Connect the supply end of the DC supply cable observing the correct polarity.
4. Connect the supply cable to the Rack Terminal Server and tighten the securing collar.
5. Switch on the supply.
6. Switch on the Rack Terminal Server.

Disconnecting your Rack Terminal Server

1. Switch off the Rack Terminal Server
2. Switch off the power source.
3. Loosen the securing collar and disconnect the supply cable to the Rack Terminal Server.
4. Disconnect the supply end of the DC supply cable (if moving the unit).
5. Disconnect attached devices.

Your Rack Terminal Server is now ready to be moved.

Appendix C Troubleshooting

You need to read this chapter if you want to...

You need to read this appendix if you want to troubleshoot problems with your Terminal Server product.

This chapter provides information on troubleshooting your Terminal Server. If you require further assistance, please contact technical support. See **Appendix B Contacting Perle**.

This appendix includes the following sections;

- **Introduction** on page **175**
- **Terminals/PC Problems** on page **176**
- **Printer Problems** on page **178**
- **Modem problems** on page **180**
- **Unit still does not communicate** on page **181**
- **Resetting Your unit** on page **182**
- **Using the Statistics screens** on page **183**
- **Using SNMP** on page **188**.
- **Diagnostics** on page **189**

Introduction

If you encounter problems when installing or using your unit, try the suggestions given in this chapter. Hopefully, the problems can be solved quickly, otherwise contact your distributor or technical support. See the following sections for further details:

- **Terminals/PC Problems** on page **176**
- **Printer Problems** on page **178**
- **Modem problems** on page **180**
- **Unit still does not communicate** on page **181**
- **Resetting Your unit** on page **182**
- **Using the Statistics screens** on page **183**
- **Using SNMP** on page **188**.

Terminals/PC Problems

If your terminal or PC connection is not working properly, symptoms are usually no output at all, 'garbage' on the screen, loss of characters or ports locking. Here is the common solution checklist to these problems:

Problem	Action required
Cable error	Replace the cable with a known good one or test the cable ends. Check the wiring against Appendix C, Cabling Guide. This is the number one problem. It is helpful to have a null modem cable and a RS-232 mini-tester.
Port settings incorrect	Check the set-ups of your unit and the terminal ensuring that they are the same at both ends. Check parity, bps rate, flow control, data bits and stop bits.
No flow control	Set flow control to be the same at both ends and ensure that the cable installed is capable of supporting it.
Port flow controlled	It is possible that an XOFF character has been received by mistakenly typing or other condition. Power the terminal off and on and type.
Wrong flow control	If the XON and XOFF characters are configurable on the terminal check that they are set to (0x11) and (0x13). If the application you are using is transferring binary data then software flow control cannot be used as some of the binary data may be interpreted as flow control characters.
Faulty terminal	Try a known working terminal on the port.
Wrong port on terminal	Many terminals have more than one port (i.e. AUX). Check that the cable has been connected to the correct port.
Faulty Server port	Try a known working terminal on the suspect port. If possible, attach a serial line monitor. If the area you are working in is prone to electrical storms, it is possible that a high voltage surge has been induced in the cable and damaged the driver/receiver chips within the unit.
Cable too long	The RS-232 specification states a maximum length of cable proportional to the bps rate. A good rule of thumb is that a 19200 bps connection should not be used on cable lengths in excess of 15m (50 ft). Also a 9600 bps signal operates reliably up to a distance of approximately 30m (100 ft). Cables of greater lengths may seem to work correctly but the connection will be less reliable.

Problem	Action required
Electrical noise	If your equipment (especially cables) is near any high voltage equipment it may be picking up electrical noise which is corrupting the data signals. Check the stats screen of the unit (check Line Stats for malformed characters). Ensure all cables are correctly screened and attempt to keep them away from high voltage equipment.
Software application error	If there are problems whenever a certain application is used then the fault may lie with the software. Check the manuals to ensure the application is configured correctly. Note that many fax packages will not work properly with remote ports.

Printer Problems

You can check some of the same problem notes in the terminal section because most are applicable to printers. The main problem is with cabling.

Problem	Action required
Testing the port	If you experience printer problems, it's a good idea to temporarily connect a terminal in place of the printer so you can ensure some of the basic functions are working correctly. Simply telnet into the communications server port: telnet elroy 10006 (port 6 on unit elroy) If the Telnet session will not connect, check the network and if you are using any of the RS-232 flow control signals, ensure they are connected correctly. If the telnet session still refuses to operate, re-configure the port for normal terminal operation and trouble-shoot again from this level. Another method is the use the test command from the CLI. This sends a continuous test pattern out to the printer. Example for port 6 (press to halt): local> test port 6 count 0 If there is no printout, check the cable or the printer.
Flow control problems	If characters disappear from the printout it may be due to a flow control problem, therefore check that the flow control is set to be the same at both ends of the cable and re-try. Alternatively, the host software may be incorrectly configured. If you are using ioland, set the debug level to a high value so that the log file will contain as much information as possible.
Configuration wrong	The first method to test this is to check the Statistics - Users Status screen. This screen should show next to the port number, the printer name (if the administrator has added it) and then the diagnostic 'Waiting for incoming connection'. If the diagnostic is something else, such as 'Connections Menu' then the port is not correctly set up and needs rechecking. Be sure to kill the port after changing its configuration.

Problem	Action required
Spooler problems	Test the printer without relying on your spooler by sending data direct to the port you created and named when you ran the ioland daemon. Do this by typing: cat data_file > /dev/laser1 If this command returns, then the Unix system believes it has sent the data and there is a good chance it has been printed successfully. This would indicate that your print spooler has not been configured properly.
ioland daemon problems	Check to see if the daemon is running. On Unix this would be: ps -ef | grep ioland This should show an ioland daemon in the table for each printer. If it isn't listed by this command, invoke it now. If it is not listed, it is probably incorrectly configured. Kill it using the Unix kill command, then run the ioland command again.

Modem problems

Check some of the same problem notes in the terminal section because most are applicable to modems. The main problem here is also cable problems and port setup.

Problem	Action required
Testing the port	The first thing to ascertain is that you can talk to the modem. Check this by telneting to the port and attempting to obtain a response from the modem. The command sequence is: telnet elroy 10006 (port 6 on unit elroy) If the modem is Hayes compatible, type the AT command and press the return key. The modem should respond with OK if the echo settings are correct at the modem. If you are unable to telnet to the port ensure that the port is set up correctly and has been killed to save the changes in configuration. Pay particular attention to flow control, monitor DSR, monitor DCD, and access field.
Modem problems	Once you have a response from the modem, dial-out to a known site and check that the correct responses are returned. Remember that modems can change their bps rate dynamically having made a connection but the unit is unable to do this. Make sure you've configured the AT string in the Remote Site Devices - Modem Configuration field. Then kill the port.

Unit still does not communicate

A situation may occur which causes the unit to completely not function. Here are possible problems

:

Problem	Action required
Port locked	Try killing the port as it may be locked due to some situation that is no longer obvious. Also, killing the port ensures that any changes in the configuration will be acted upon.
Power cycling	Power cycle the device connected (if this is possible) as it may be that it has locked, or the set-up within the device is in error. Also try power cycling the unit itself.
Network errors	Try 'pinging' the unit to establish connection.
Network cable problems	Check the network cable again. Does it work on another node correctly. Is the BNC (or AUI) connector fitted correctly?
Configuration problems	Check the IP address again on the Server Menu.
Power problems	Is the green LED power light on? Check the power itself with the plug, wall socket, fuses, etc. Is the green LED power light dim? Call your supplier or technical support.
Hardware problems	If all three network LEDs are flashing continuously on/off at approx 4Hz. this may point to a memory fail test. Call your supplier or technical support.

Resetting Your unit

At times, a support problem may require you to reset or diagnose your unit. It is best to discuss this matter with your supplier or technical support.

You can perform a factory reset using either of the following methods

Using "facreset" command

1. Power on the unit and type the following from a CLI session:

   Local> su

   Password> iolan

   ADMIN:Local> facreset

   Do you really want to do this (y/n) [n] ? y

   Performing factory reset ...

Using Diagnostic menu reset

1. Connect a serial terminal (configured for 9600,n,8,1) to port 1 of the server.
2. Power on the server and press "<cntrl> B" on the terminal five times in succession while the unit LEDs are flashing (the firmware decompression phase).

   The diagnostic menu is now displayed on the terminal.

> Note
>
> If you have an older unit with a reset button, to display the Diagnostic Menu proceed as follows;
>
> a. Press and hold down the reset button.
> b. Power on your Terminal Server server unit.
>
> The Diagnostic menu now appears.
>
> c. Release the reset button.

3. Within the diagnostic menu, select the following options:

   5. Reset

   1. Reset all settings to factory defaults

   q. Quit and boot server firmware

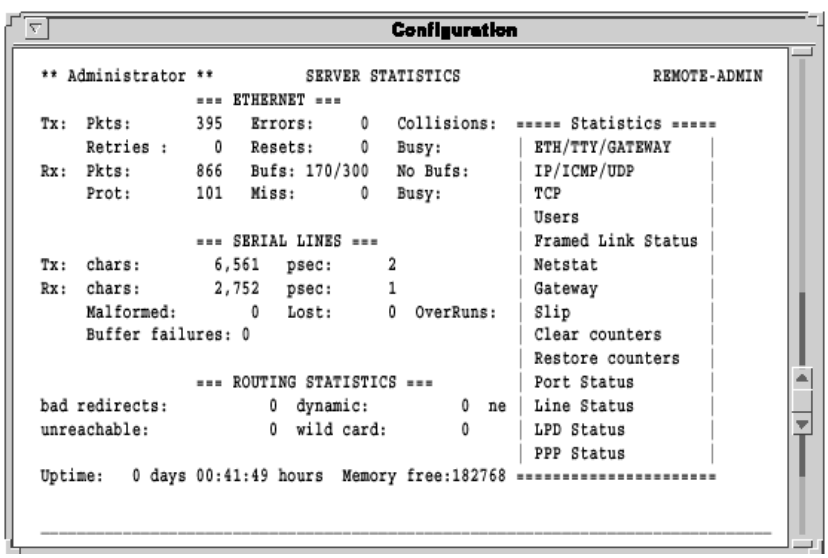
After this is done, the unit should start sending BOOTP request packets. This procedure is useful for factory defaulting units which cannot be reached by TCP/IP. This includes reassigning a programmed unit to a network to which the previously assigned IP address does not belong.

Using the Statistics screens

Your unit maintains a large number of statistics and these are available on several statistics screens. The various screens and the meanings of the statistics are described in this section. These screens are used along with technical support in troubleshooting. Only the most significant entries will be reviewed in this section.

Initial entry to all statistics screens is achieved from the ETH/TTY/Routing - Gateway - Statistics screen, which is reached by selecting stats from the Administration Menu (the CLI mode can also be used with the show command).

Once this screen has been displayed the Gateway - Statistics pop-up menu is obtained by pressing the Enter key.



All of the statistics screens are now accessible through this Statistics pop-up menu. Pressing in any of the statistics screens displays the same pop-up menu.

A summary of each is provided and then the most important screens are briefly described:

ETH/TTY/GATEWAY

This is a general overview of Ethernet activity, serial activity

and gateway stats. It shows characters passed and uptime.

IP/ICMP/UDP

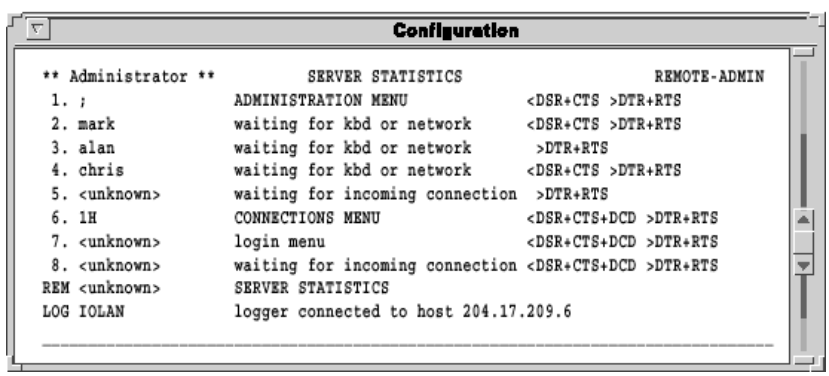
This is a comprehensive screen of networking protocol stats for IP, ICMP and UDP. You can identify bad IP packets coming in from your network.

TCP

This is a comprehensive screen of TCP protocol stats. You can identify bad TCP packets coming in from your network.

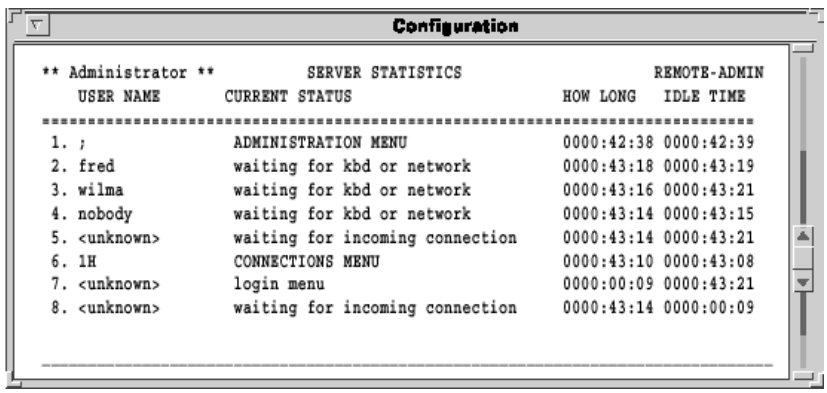
Users

This is a good menu for showing port and control signal status. You can identify status on each ports control signals.



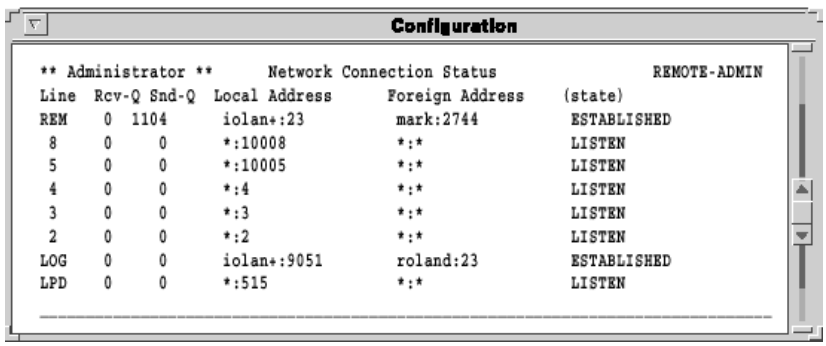
Framed Link Status

This is a good menu for Internet Service Providers especially. It shows who is logged on, current port status, which hosts are connected, and how long the port has been in its current state and its idle time.



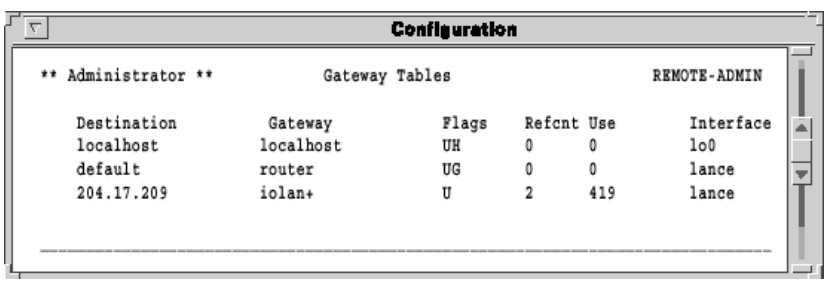
Netstat

This is a good menu for determining TCP connection status and the port access status.



Gateway

This is an often used screen for determining routing problems.



SLIP

This is a comprehensive SLIP stat and streams buffer screen.

Clear counters

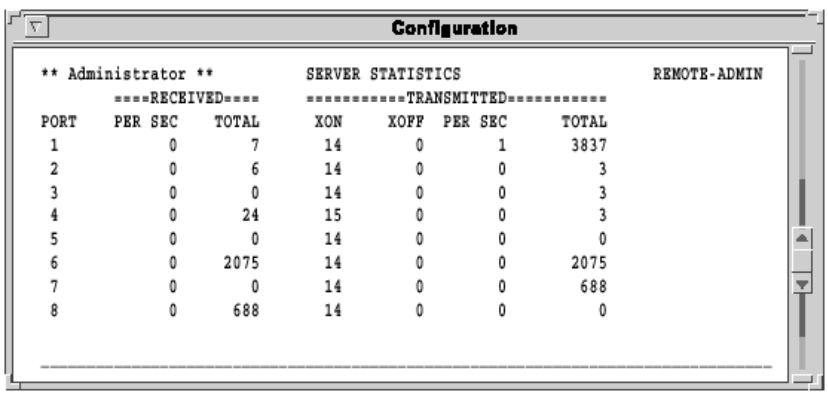
This function sets all of the displayed counters to zero.

Restore counters

The counter totals are redisplayed.

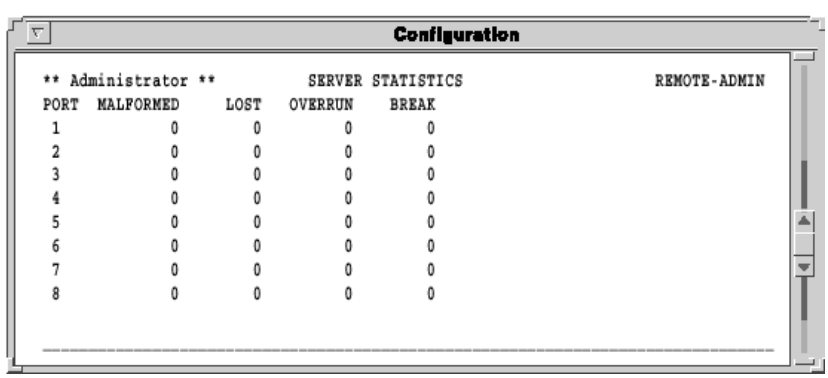
Port Status

This is a good screen for viewing individual port activity.



Line status

This is a good screen for spotting baud rate and parity errors which if malformed is rapidly incrementing.



LPD Status

This screen allows you to check the status of your LPD connections and print queues.

PPP Status

This shows the PPP negotiation progress status and established PPP connections.

Using SNMP

SNMP stands for Simple Network Management Protocol. A full description of SNMP is beyond the scope of this manual. However, if you're familiar with SNMP, you can use this as a troubleshooting tool. As the name suggests SNMP is a protocol designed to allow control of a whole network. The provides an SNMP agent, this means that it responds to SNMP requests. It does not have the facility to generate SNMP requests to monitor another system.

A host machine running the client SNMP package can request any of the defined variables. It can also set a limited number of the communications server variables thus allowing configuration of the unit to be done remotely. The SNMP trap function is set up using the Trap function screen. This is accessed from the Administration Menu.

Diagnostics

Entering the Diagnostic Menu

1. Connect a serial terminal (configured for 9600,n,8,1) to port 1 of the server.
2. Power on the server and press "<cntrl> B" on the terminal five times in succession while the unit LEDs are flashing (the firmware decompression phase).

> Note
>
> If you have an older unit with a reset button, to display the Diagnostic Menu proceed as follows;
>
> a. Press and hold down the reset button.
> b. Power on your Terminal Server server unit.
> The Diagnostic menu now appears.
> c. Release the reset button.

This causes the following menu to be displayed on the terminal:

1. Self-test.
2. Diagnostics.
3. Monitor.
4. Download.
5. Reset.

q Quit and boot server firmware.

Self-test

This is an option intended for use at the factory and by repair centres, all of the functionality provided by this test is available by selecting the Diagnostics option. It is recommended that you do not select the Self-test option.

Monitor

This option allows a number of settings to be made and allows read and write operations directly into specified memory locations. Again it is not intended for use outside of the factory or repair centres.

Download

It is possible that when trying to download a new version of firmware over the network that when the FLASH is being programmed it can become corrupt. In the unlikely event of FLASH corruption it is possible to download new firmware via the FLASH bootstrap code.

Ethernet Interface

You will be prompted to accept or change the following parameters:

Server Ethernet address.

Server IP address.

Host IP address (from which the download file will come).

Full path and file name of the down-loadable firmware file.

When the settings have been correctly entered the type of Ethernet interface required can be set, this needs to be selected manually and will not be configured automatically.

Also note that this feature is a backup and normally firmware should be downloaded using the options included in the firmware itself, allowing updates etc. to be downloaded from anywhere on the network.

Ensure the server and host are on the same physical network. The bootstrap code does not support routing.

Reset

This allows the user to reset a number or all of the settings stored in FLASH which constitute the server's configuration.

The following settings may be reset:

1. Reset all settings to factory defaults.
2. Reset password.
3. Reset IP address.
4. Reset product name.
5. Reset Ethernet address.

q Quit.

Reset all settings

This clears the entire permanent database in FLASH. When the server runs the firmware it will report a permanent database error and set all of the configurations to their default settings.

Reset password

This is useful if the password is lost or forgotten, it will set the password back to iolan.

Reset IP address

This will reset the IP address of the communications server.

Reset product name

This option changes the name displayed in the bottom left corner of the menu screen, it is not intended for use outside the factory.

Reset Ethernet address

Do not attempt to enter the Ethernet address unless the unit's configuration has become completely corrupt. The Ethernet address is recorded on the base of the unit and should never be changed.

Quit

This will exit the bootstrap menu and cause the firmware stored in FLASH to be booted.

Appendix D Cabling

You need to read this chapter if you want to...

You need to read this appendix if you want cabling information for your Terminal Server product.

This appendix provides cabling and connector information about the Black Box Terminal Server including serial ports and cables for various applications.

This chapter includes the following sections;

- **Introduction** on page **194**
- **Serial port connectors on the Terminal Server unit** on page **195**
- **Standard modem cables** on page **199**
- **Standard Terminal/PC cables** on page **201**
- **Printer cables with hardware flow control** on page **205**

Introduction

The following guide describes pinouts and cables for the Terminal Server (DB25), Rack Terminal Server(RJ45) and 102/104 Terminal Server (RJ45) units. Both versions equipped with RJ45 connectors are also available as RS-422 units.

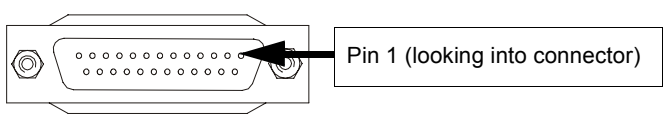
Any cable you use should be shielded to comply with FCC requirements. Be careful not to run data cables near fluorescent lights, electric motors or other sources of electrical noise. Maximum cable lengths for RS-232 are specified at 60m (200 feet) but are proportional to baud rates - the higher the baud, the smaller the cable should be. A good rule of thumb is that a 19200 bps connection should not be used on cable lengths in excess of 15m (50 feet). Also, a 9600 bps signal operates reliably up to a distance of approximately 30m (100 feet). Cables of greater lengths may seem to work correctly but the connection will be less reliable. For reliable RS-422 operation, signal ground must be connected at both ends of the cable. Maximum cable length is 1.2 km but at 115.2 kbs it is reduced to 1 km.

Serial port connectors on the Terminal Server unit

Serial port connector guide

Product	Serial port connector type	For details see...
Terminal Server	DB25 female	**RS232 DB25 female DTE** on page **195**.
Rack Terminal Server RS232	RJ45 female	**RS232 RJ45 DTE socket** on page **197**.
Rack Terminal Server RS422	RJ45 female	**RS422 RJ45 DTE socket** on page **198**.
102/104 Terminal Server RS232	RJ45 female	**RS232 RJ45 DTE socket** on page **197**.
102/104 Terminal Server RS422	RJ45 female	**RS422 RJ45 DTE socket** on page **198**.

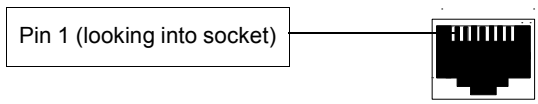
RS232 DB25 female DTE



Pin	Signal	Direction	Description
1	GND		Protective ground
2	TXD	Out	Transmit Data
3	RXD	In	Receive Data
4	RTS	Out	Request To Send
5	CTS	In	Clear To Send
6	DSR	In	Data Set Ready

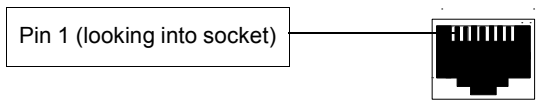
Pin	Signal	Direction	Description
7	S/GND		Signal ground
8	DCD	In	Data Carrier Detect
20	DTR	Out	Data Terminal Ready

RS232 RJ45 DTE socket



Pin	Signal	Direction	Description
1	DCD	In	Data Carrier Detect
2	RTS	Out	Request To Send
3	DSR	In	Data Set Ready
4	TXD	Out	Transmit Data
5	RXD	In	Receive Data
6	S/GND		Signal ground
7	CTS	In	Clear To Send
8	DTR	Out	Data Terminal Ready

RS422 RJ45 DTE socket



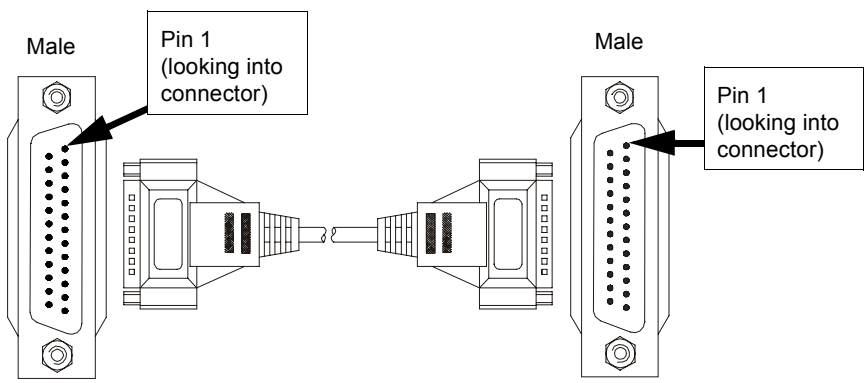
Pin	Signal	Direction	Description
1			No connection
2	S/GND		Signal ground
3	RXA	In	Receive Data A
4	TXA	Out	Transmit Data A
5	TXB	Out	Transmit Data B
6	RXB	In	Receive Data B
7			No connection
8	S/GND		Signal ground

Standard modem cables

Terminal Server DB25 DTE to Modem DB25 DCE

Typical uses This type of cable is used to connect to DCE devices such as Modems.

Cable diagram



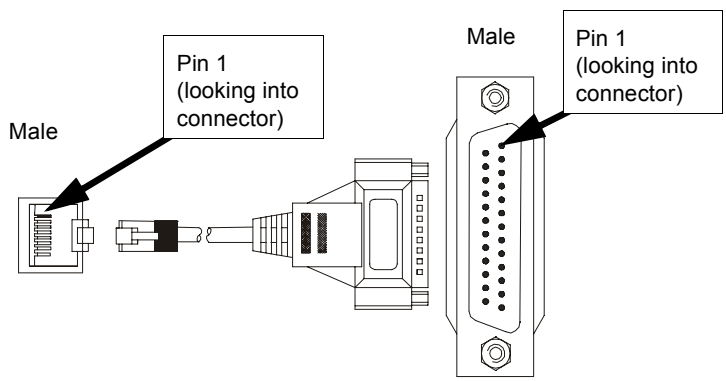
Connector pinout table

DB25 (Terminal Server)				DB25 (MODEM)		
Pin	**Signal**	**Direction**	**Description**	**Pin**	**Signal**	**Description**
1	Chassis		Chassis ground	1	Chassis	Chassis ground
2	TXD	Out	Transmit Data	2	TXD	Transmit Data
3	RXD	In	Receive Data	3	RXD	Receive Data
4	RTS	Out	Request To Send	4	RTS	Request To Send
5	CTS	In	Clear To Send	5	CTS	Clear To Send
6	DSR	In	Data Set Ready	6	DSR	Data Set Ready
7	GND		Ground	7	GND	Ground
8	DCD	In	Data Carrier Detect	8	DCD	Data Carrier Detect
20	DTR	Out	Data Terminal Ready	20	DTR	Data Terminal Ready

Rack Terminal Server and 102/104 Terminal Server RS232 RJ45 DTE to Modem DB25 DCE

Typical uses This type of cable is used to connect to DCE devices such as Modems.

Cable diagram



Connector pinout table

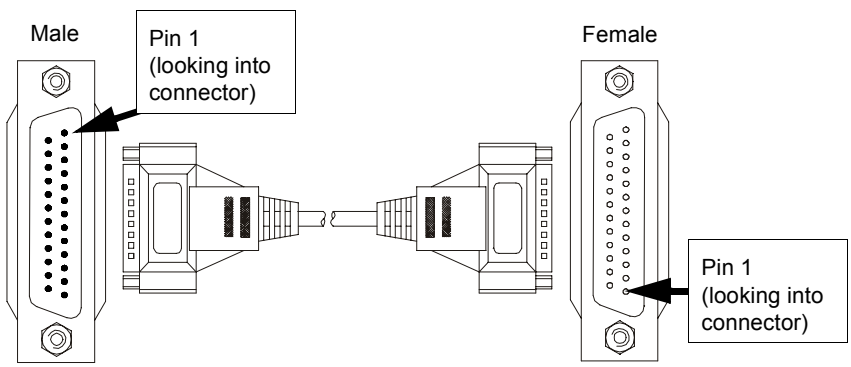
RJ45 (Terminal Server)				DB25(MODEM)		
Pin	**Signal**	**Direction**	**Description**	**Pin**	**Signal**	**Description**
1	DCD	In	Data Carrier Detect	8	DCD	Data Carrier Detect
2	RTS	Out	Request To Send	4	RTS	Request To Send
3	DSR	In	Data Set Ready	6	DSR	Data Set Ready
4	TXD	Out	Transmit Data	2	TXD	Transmit Data
5	RXD	In	Receive Data	3	RXD	Receive Data
6	S/GND		Signal ground	7	S/GND	Signal ground
7	CTS	In	Clear To Send	5	CTS	Clear To Send
8	DTR	Out	Data Terminal Ready	20	DTR	Data Terminal Ready

Standard Terminal/PC cables

Terminal Server DB25 DTE to Terminal DB25 DTE

Typical uses This type of cable is used to connect to DTE devices such as Terminals/PCs.

Cable diagram



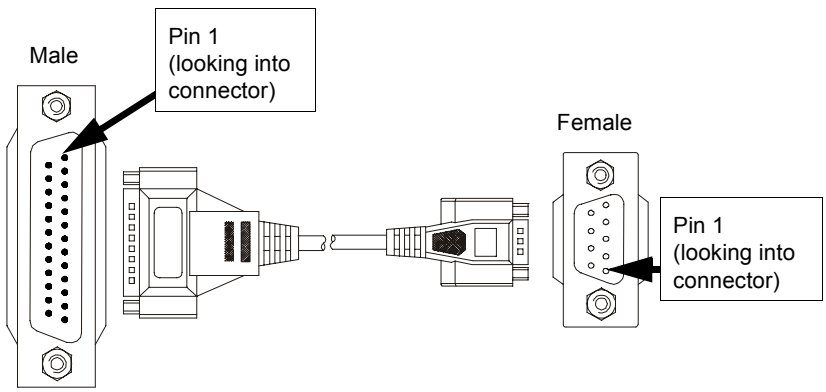
Connector pinout table

DB25 (Terminal Server)				DB25 (Terminal)		
Pin	**Signal**	**Direction**	**Description**	**Pin**	**Signal**	**Description**
2	TXD	Out	Transmit Data	3	RXD	Receive Data
3	RXD	In	Receive Data	2	TXD	Transmit Data
7	GND		Ground	7	GND	Ground

Terminal Server DB25 DTE to PC DB9 DTE

Typical uses This type of cable is used to connect to DTE devices such as Terminals/PCs.

Cable diagram



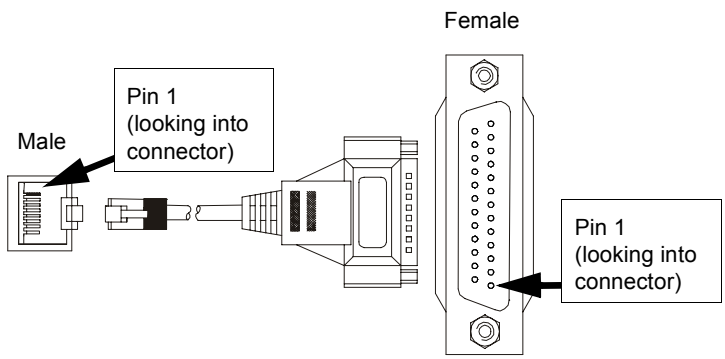
Connector pinout table

DB25 (Terminal Server)				DB9 (Terminal)		
Pin	**Signal**	**Direction**	**Description**	**Pin**	**Signal**	**Description**
2	TXD	Out	Transmit Data	2	RXD	Receive Data
3	RXD	In	Receive Data	3	TXD	Transmit Data
7	GND		Ground	5	GND	Ground

Rack Terminal Server and 102/104 Terminal Server RJ45 DTE to Terminal DB25 DTE

Typical uses This type of cable is used to connect to DTE devices such as Terminals/PCs.

Cable diagram



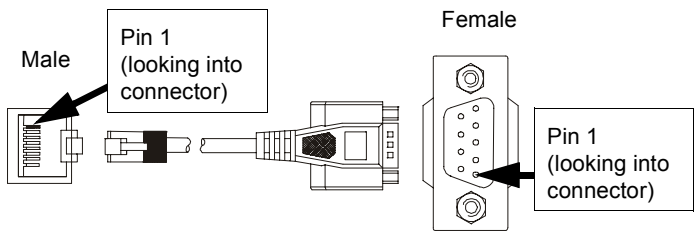
Connector pinout table

RJ45 (Terminal Server)				DB25 (Terminal)		
Pin	**Signal**	**Direction**	**Description**	**Pin**	**Signal**	**Description**
4	TXD	Out	Transmit Data	2	RXD	Receive Data
5	RXD	In	Receive Data	3	TXD	Transmit Data
6	GND		Ground	7	GND	Ground

Rack Terminal Server and 102/104 Terminal Server RJ45 DTE to PC DB9 DTE

Typical uses This type of cable is used to connect to DTE devices such as PCs.

Cable diagram



Connector pinout table

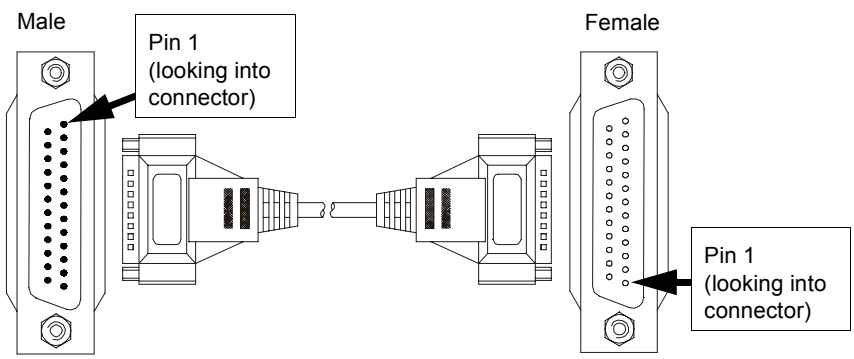
RJ45 (Terminal Server)				DB9 (PC)		
Pin	**Signal**	**Direction**	**Description**	**Pin**	**Signal**	**Description**
4	TXD	Out	Transmit Data	2	RXD	Receive Data
5	RXD	In	Receive Data	3	TXD	Transmit Data
6	GND		Ground	5	GND	Ground

Printer cables with hardware flow control

Terminal Server DB25 DTE to Printer DB25 DTE

Typical uses This type of cable is used to connect to DTE devices such as PCs.

Cable diagram



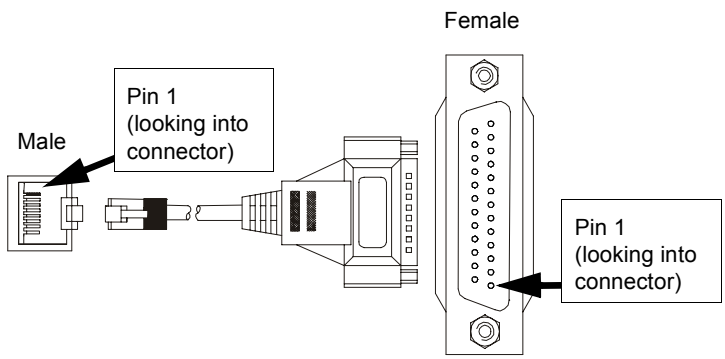
Connector pinout table

DB25 (Terminal Server)				DB25 (Printer)		
Pin	**Signal**	**Direction**	**Description**	**Pin**	**Signal**	**Description**
2	TXD	Out	Transmit Data	3	RXD	Receive Data
3	RXD	In	Receive Data	2	TXD	Transmit Data
5	CTS	In	Clear To Send	20	DTR	Data Terminal Ready
7	GND		Ground	7	GND	Ground

Rack Terminal Server and 102/104 Terminal Server RJ45 male to printer DB25 DTE

Typical uses This type of cable is used to connect to DTE devices such as PCs.

Cable diagram



Connector pinout table

RJ45 (Terminal Server)				DB25 (Printer)		
Pin	**Signal**	**Direction**	**Description**	**Pin**	**Signal**	**Description**
4	TXD	Out	Transmit Data	2	RXD	Receive Data
5	RXD	In	Receive Data	3	TXD	Transmit Data
6	GND		Ground	7	GND	Ground
7	CTS	In	Clear To Send	20	DTR	Data Terminal Ready

Index

Numerics

48V DC, Terminal Server variant 169

A

about this manual 5
access menu 137
Address Resolution Protocol 35
administration menu 135
ARP
    communicating with 35
arp 161
    command 161
authentication
    of host 71
    of logging 73

C

cables 193
    modems 199
    pc 201
    printer 205
    terminal 201
cabling 193
clear command 161
CLI 156
    using 158
client login 64
command line interface 156
    using 158
commands 156
    arp 161
    clear 161
    connect 161
    copy 162
    descriptions of 161
    dial 162
    disconnect 162
    exit 162
    facreset 162
    gateway 162
    help 163
    host 163
    kill 163
    lock 163
    logout 163
    prov 163
    reboot 164
    resume 164
    rlogin 164
    save 164
    set 165
    show 167
    su 167
    telnet 167
    test 168
communicating
    via pc 36
    via terminal 36
connect command 161
connecting to network 33
connections
    making on multi-user systems 55
connections menu 124
connector pinouts 193
copy 162
copy command 162

D

dial command 162
dial-in modem ports, setting up 58
dial-in port 60
dialout modem ports
    configuration 77
    host 78

remote access systems 80
remote site devices 83
routing 79
setup 75
disconnect 162
disconnect command 162

E

exit command 162

F

facreset 162
facreset command 162
factory defaults
restoring 162

G

gateway
command 162
menu 145

H

help command 163
host 62
address menu 146
authentication 71
command 163
table
setting up 54

I

installation 32
installing
the unit 32
ioland 114
printing with 96

K

kill command 163

L

lines menu 147
lock commands 163
logging
authentication 73
logout command 163
LPD printing 99

M

menu system 37
menus 37, 121
access 137
administration 135
connections 124
gateway 145
host address 146
introduction to 122
lines 147
password options 144
port 150
port setup 126
quit command 150
reboot command 150
server configuration 151
statistics screens 154
trap function 155
modem 63
authentication and logging
host 71
logging 73
user authentication 68
cables 199
dialout ports
configuration of 77
host 78
remote access systems 80
remote site devices 83
routing 79
setup 75
virtual 85, 87, 93
modem, authentication and logging 66
multi-user systems
connecting 55
connecting to 51

host table 54
setting up 50

N

network, connecting to 33

P

password options, changing 144
pc
cables 201
communicating with 36
port configuration
for terminals 52
port menu 150
port setup menu 126
printer cables 205
printing 94
using ioland 96
using LPD 99
using RCP 105
prov command 163

Q

quit command 150

R

RCP printing 105
reboot command 150, 164
reset
button, on legacy units 182
procedure for 182
procedure for legacy units 182
resume command 164
reverse telnet 112
rlogin command 164
routing dialout 79

S

save command 164
serial ports, connectors 195
server configuration menu 151
set commands 165
show command 167
statistics screens 154
su command 167
switching on 34

T

telnet command 167
terminal
communicating with 36
terminal cables 201
terminal port configuration 52
Terminal Server
48V DC variant 169
terminals
on multi-user systems 50
test command 168
trap function 155
troubleshooting 174

V

virtual modem 85
AT commands 93
configuring ports for 87
vmodem 85
AT commands 93
configuring ports for 87
resposnses 92

© Copyright 2002. Black Box Corporation. All rights reserved.

1000 Park Drive • Lawrence, PA 15055-1018 • 724-746-5500 • Fax 724-746-0746