



December 2016

Terminal Servers - LES4011 to 14

Terminal Server User Guide

Version 4.8

5500182-48

CUSTOMER Order **toll-free** in the U.S 24 hours, 7 A.M. Monday to midnight Friday: **877-877-BBOX**
SUPPORT FREE technical support, 24 hours a day, 7 days a week: Call **724-746-5500** or fax **724-746-0746**
INFORMATION 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 debe ser situado fuera del alcance de fuentes de calor como radiadores, registros de calor, estufas u otros aparatos (incluyendo amplificadores) que producen calor.
11. El aparato eléctrico deberá ser conectado a una fuente de poder sólo del tipo descrito en el instructivo de operación, o como se indique en el aparato.
12. Precaución debe ser tomada de tal manera que la tierra física y la polarización del equipo no sea eliminada.
13. Los cables de la fuente de poder deben ser guiados de tal manera que no sean pisados ni pellizcados por objetos colocados sobre o contra ellos, poniendo particular atención a los contactos y receptáculos donde salen del aparato.
14. El equipo eléctrico debe ser limpiado únicamente de acuerdo a las recomendaciones del fabricante.
15. En caso de existir, una antena externa deberá ser localizada lejos de las líneas de energía.
16. El cable de corriente deberá ser desconectado del cuando el equipo no sea usado por un largo periodo de tiempo.
17. Cuidado debe ser tomado de tal manera que objetos líquidos no sean derramados sobre la cubierta u orificios de ventilación.
18. Servicio por personal calificado deberá ser provisto cuando:
 - a. El cable de poder o el contacto ha sido dañado; u
 - b. Objetos 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.

FCC Requirements for Telephone-Line Equipment

1. The Federal Communications Commission (FCC) has established rules which permit this device to be directly connected to the telephone network with standardized jacks. This equipment should not be used on party lines or coin lines.
2. If this device is malfunctioning, it may also be causing harm to the telephone network; this device should be disconnected until the source of the problem can be determined and until the repair has been made. If this is not done, the telephone company may temporarily disconnect service.
3. If you have problems with your telephone equipment after installing this device, disconnect this device from the line to see if it is causing the problem. If it is, contact your supplier or an authorized agent.
4. The telephone company may make changes in its technical operations and procedures. If any such changes affect the compatibility or use of this device, the telephone company is required to give adequate notice of the changes.
5. If the telephone company requests information on what equipment is connected to their lines, inform them of:
 - a. The telephone number that this unit is connected to.
 - b. The ringer equivalence number.
 - c. The USOC jack required: RJ-11C.
 - d. The FCC registration number.

Items (B) and (D) can be found on the unit's FCC label. The ringer equivalence number (REN) is used to determine how many devices can be connected to your telephone line. In most areas, the sum of the RENs of all devices on any one line should not exceed five. If too many devices are attached, they may not ring properly.

6. In the event of an equipment malfunction, all repairs should be performed by your supplier or an authorized agent. It is the responsibility of users requiring service to report the need for service to the supplier or to an authorized agent.

Certification Notice for Equipment Used in Canada

The Industry Canada label identifies certified equipment. This certification means that the equipment meets certain telecommunications-network protective, operation, and safety requirements. Industry Canada does not guarantee the equipment will operate to the user's satisfaction.

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. In some cases, the company's inside wiring associated with a single-line individual service may be extended by means of a certified connector assembly (extension cord). The customer should be aware that compliance with the above conditions may not prevent degradation of service in some situations.

Repairs to certified equipment should be made by an authorized maintenance facility—in this case, Black Box. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment.

Users should ensure for their own protection that the electrical ground connections of the power utility, telephone lines, and internal metallic water pipe system, if present, are connected together. This precaution may be particularly important in rural areas.

CAUTION: Users should not attempt to make such connections themselves, but should contact the appropriate electric inspection authority, or electrician, as appropriate.

The LOAD NUMBER (LN) assigned to each terminal device denotes the percentage of the total load to be connected to a telephone loop which is used by the device, to prevent overloading.

The termination on a loop may consist of any combination of devices, subject only to the requirement that the total of the load numbers of all the devices does not exceed 100.

FEDERAL COMMUNICATIONS COMMISSION AND INDUSTRY CANADA RADIO FREQUENCY INTERFERENCE STATEMENTS

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

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

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

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

Table of Contents

Preface	15
About This Book	15
Intended Audience	15
Documentation	15
Typeface Conventions	16
Online Help	16
Chapter 1 Introduction	17
About the Terminal Server	17
Terminal Server Models	17
Terminal Server Features	18
Hardware	18
Software	19
Accessing the Terminal Server	19
General Features	19
Security	19
Chapter 2 Hardware and Connectivity	20
Introduction	20
Terminal Server Components	20
What's Included	20
What You Need to Supply	20

Power Supply Specifications	20
Desktop Models	20
Getting to Know Your Terminal Server	21
Overview	21
Terminal Server 1-Port	21
Console/Serial Switch	22
Console Mode	22
Serial Mode	22
Powering Up the Terminal Server	23
Serial Only Models	23
Chapter 3 Configuration Methods	24
Introduction	24
Configuration Methods Overview	24
Configures an IP Address	24
Requires a Configured IP Address	25
Easy Config Wizard	26
DeviceManager	27
Overview	27
Access Platforms	27
Unique Features	27
Connecting to a Terminal Server Using DeviceManager	27
Using DeviceManager	29
WebManager	30
Overview	30
Access Platforms	30
Unique Features	30
Connecting to a Terminal Server Using WebManager	30
Command Line Interface	31
Overview	31
Access Platforms	31
Unique Features	32

Connecting to a Terminal Server Using the CLI	32
Through the Network.....	32
Through the Serial Port	32
Using the CLI	32
Menu.....	33
Overview.....	33
Access Platforms	33
Unique Features	33
Connecting to the Terminal Server Using the Menu	33
Using the Menu	33
DHCP/BOOTP	34
Overview.....	34
Unique Features	34
Connecting to the Terminal Server Using DHCP/BOOTP	34
Using DHCP/BOOTP.....	34
DHCP/BOOTP Parameters	35
SNMP.....	35
Overview.....	35
Access Platforms	35
Unique Features	35
Connecting to the Terminal Server Using SNMP	36
Using the SNMP MIB	36
Chapter 4 Getting Started	38
Introduction	38
Easy Configuration Wizard	38
Setting Up the Network	39
Using DeviceManager	39
Using WebManager	40
Using a Direct Serial Connection to Specify an IP Address.....	40
Using a Direct Serial Connection to Enable BOOTP/DHCP	41
Using ARP-Ping.....	42
For an IPv6 Network	42

Setting Up the Serial Port(s)	43
Setting Up Users	45
Chapter 5 Using DeviceManager and WebManager.....	46
Introduction	46
Navigating DeviceManager/WebManager	47
DeviceManager	47
WebManager	48
Using DeviceManager to Connect to the Terminal Server	49
Starting a New Session	49
Assigning a Temporary IP Address to a New Terminal Server	50
Adding/Deleting Manual Terminal Servers	51
Logging in to the Terminal Server	51
Using WebManager to Connect to the Terminal Server	52
Logging into the Terminal Server	52
Configuration Files	53
Creating a New Terminal Server Configuration in DeviceManager ...	53
Opening an Existing Configuration File	53
Importing an Existing Configuration File	53
Managing the Terminal Server.....	53
Chapter 6 Configuring Serial Ports	54
Introduction	54
Serial Ports	54
Overview.....	54
Functionality	54
Editing a Serial Port	55
Resetting a Serial Port	56
Serial Port Profiles	57
Common Tabs.....	57
Overview	57
Hardware Tab Field Descriptions.....	57

Packet Forwarding Tab Field Descriptions	60
Console Management Profile	62
Overview	62
Functionality	62
General Tab Field Descriptions.....	63
Advanced Tab Field Descriptions	64
COMredirect Profile.....	67
Overview	67
Functionality	67
General Tab Field Descriptions.....	68
Adding/Editing Additional COMredirect Hosts.....	69
Adding/Editing a Multihost Entry	70
Advanced Tab Field Descriptions	71
TCP Sockets Profile	73
Overview	73
Functionality	73
General Tab Field Descriptions.....	74
Adding/Editing Additional Hosts	76
Adding/Editing a Multihost Entry	77
Advanced Tab Field Descriptions	78
UDP Sockets Profile	81
Overview	81
Functionality	81
General Tab Field Descriptions.....	84
Terminal Profile	86
Overview	86
Functionality	86
General Tab Field Descriptions.....	86
Advanced Tab Field Descriptions	88
User Service Settings.....	90
Login Settings	90
Telnet Settings	90
Serial Tunneling Profile	92
Overview	92
Functionality	92
General Tab Field Descriptions.....	93
Advanced Tab Field Descriptions	94
Virtual Modem Profile.....	95
Overview	95
Functionality	95
General Tab Field Descriptions.....	96
Advanced Tab Field Descriptions	97
Phone Number to Host Mapping.....	100
VModem Phone Number Entry	100

Modbus Gateway Profile.....	102
Overview	102
Functionality	102
General Tab Field Descriptions.....	103
Advanced Field Descriptions.....	104
Modbus Slave IP Settings Field Descriptions	105
Adding/Editing Modbus Slave IP Settings.....	105
Modbus Slave Advanced Settings Field Descriptions.....	107
Advanced.....	108
Advanced Serial Settings Tab	108
Overview	108
Field Descriptions.....	108
Modems Tab.....	109
Overview	109
Adding/Editing a Modem	110
COMredirect Baud Rate Tab.....	111
Overview	111
Functionality	111
Field Definitions.....	111
Chapter 7 Network Settings	112
Introduction	112
IP Settings	113
IPv4 Settings	113
Overview	113
Field Descriptions.....	113
IPv6 Settings	114
Overview	114
Field Descriptions.....	114
Adding/Editing a Custom IPv6 Address	115
Field Descriptions.....	115
Advanced	116
Overview	116
Field Descriptions.....	116
Advanced.....	117
Host Table	117
Overview	117
Functionality	117
Field Descriptions.....	117

Adding/Editing a Host	117
Route List	118
Overview	118
Functionality	118
Field Descriptions.....	118
Adding/Editing Routes	119
Chapter 8 Configuring Users	120
Introduction	120
User Settings	121
Overview.....	121
Functionality	121
Adding/Editing Users	122
General Tab	122
Overview	122
Functionality	122
Field Descriptions.....	122
Services Tab	124
Overview	124
Functionality	124
Field Descriptions.....	124
Advanced Tab	125
Overview	125
Field Descriptions.....	125
Sessions Tab	126
Overview	126
Functionality	126
Field Descriptions.....	127
Serial Port Access Tab	128
Overview	128
Field Descriptions.....	128
Chapter 9 Configuring Security	129
Introduction	129
Services	129
Overview.....	129
Functionality	129

Field Descriptions	130
Chapter 10 Configuring the System	131
Introduction	131
Alerts	131
Syslog	131
Overview	131
Field Descriptions.....	131
Management	132
SNMP	132
Overview	132
Field Descriptions.....	132
Field Descriptions.....	133
Advanced	134
Overview	134
Login Tab Field Descriptions.....	134
Startup Files Tab Field Descriptions	135
Message of the Day (MOTD) Tab Field Descriptions	136
TFTP Tab Field Descriptions	137
Chapter 11 System Administration.....	138
Introduction	138
Managing Configuration Files	138
Saving Configuration Files	138
Downloading Configuration Files	138
Downloading Configuration Files to Multiple Terminal Servers	139
Uploading Configuration Files	139
Specifying a Custom Factory Default Configuration	140
Resetting to the Original Factory Default Configuration	140
Downloading Terminal Server Firmware	141
Setting the Terminal Server's Date and Time.....	141
Rebooting the Terminal Server.....	141
Resetting the serial port statistics	142
Resetting the Terminal Server to Factory Defaults	142

Language Support	142
Loading a Supplied Language	142
Translation Guidance.....	143
Software Upgrades and Language Files	143
Downloading Terminal Definitions	144
Creating Terminal Definition Files	144
Resetting Configuration Parameters	145
Lost Admin Password	146
Appendix A Virtual Modem AT Commands	147
Virtual Modem Initialization Commands	147
Appendix B Pinouts and Cabling Diagrams	149
Serial Pinouts	149
DB25 Male	149
DB25 Female	150
RJ45.....	151
DB9 Male	152
EIA-232 Cabling Diagrams	153
Terminal DB25 Connector	153
DB25 Male	153
DB25 Female	153
RJ45.....	154
DB9 Male	154
Modem DB25 Connector.....	155
DB25 Male	155
RJ45.....	155
DB9 Male	156
Appendix C Setting Jumpers	157
Introduction	157
1-Port Terminal Server.....	157
Terminal Server DB25 Male/Female.....	157
Terminal Server RJ45	158
Terminal Server DB9.....	158

Appendix D COMredirect Utility	159
Introduction	159
COMredirect	159
Appendix E Troubleshooting	160
Introduction	160
Hardware Problems	160
Communication Issues.....	160
DeviceManager Problems	161
Host Problems.....	161
Login Problems	161
Problems with Terminals	162
Unknown IP Address	162
DHCP/BOOTP Problems.....	163
Language Problems.....	163
Long Reboot Cycle	163
IPv6 Issues	163
Glossary	164
Appendix G Data Logging	166
Introduction	166
COMredirect Profile	166
TCP Socket Profile.....	166
Appendix H Modbus ReMapping	167
Configuring the Modbus UID Translation Feature	168
Index	169

Preface

About This Book

This guide provides the information you need to:

- configure the Terminal Server.
- incorporate the Terminal Server into your production environment.

Intended Audience

This guide is for administrators who will be configuring the Terminal Server.

Some prerequisite knowledge is needed to understand the concepts and examples in this guide:

- If you are using an external authentication application(s), working knowledge of the authentication application(s).
- Knowledge of TFTP, the transfer protocol the Terminal Server uses.

Documentation

The following documentation is included on the Terminal Server installation CD:



- *BLACK BOX® 1-Port Quick Start Guide*
- *BLACK BOX® 2-4-Port Desktop Quick Start Guide*
- *BLACK BOX® Rack Mount Quick Start Guide*
- *BLACK BOX® Terminal Server User Guide*
- *BLACK BOX® Terminal Server Command Line Reference Guide*
- *BLACK BOX® COMredirect Windows® User Guide*
- *BLACK BOX® COMredirect Linux User Guide*
- *BLACK BOX® COMredirect Solaris User Guide*
- *BLACK BOX® COMredirect Unixware User Guide*
- *BLACK BOX® COMredirect SCO Openserver 5 User Guide*
- *BLACK BOX® COMredirect SCO Openserver 6 User Guide*
- *BLACK BOX® COMredirect HP-UX User Guide*
- Online Help in the DeviceManager (automatically installed with the DeviceManager application)

Typeface Conventions

Most text is presented in the typeface used in this paragraph. Other typefaces are used to help you identify certain types of information. The other typefaces are:

Typeface Example	Usage
At the C: prompt, type: <code>add host</code>	This typeface is used for code examples and system-generated output. It can represent a line you type in, or a piece of your code, or an example of output.
Set the value to TRUE .	The typeface used for TRUE is also used when referring to an actual value or identifier that you should use or that is used in a code example.
<code>subscribe <i>project</i> <i>subject</i></code> <code>run <i>yourcode</i>.exec</code>	The italicized portion of these examples shows the typeface used for variables that are placeholders for values you specify. This is found in regular text and in code examples as shown. Instead of entering <i>project</i> , you enter your own value, such as <code>stock_trader</code> , and for <i>yourcode</i> , enter the name of your program.
File, Save	This typeface and comma indicates a path you should follow through the menus. In this example, you select Save from the File menu.
<i>BLACK BOX® User Guide</i>	This typeface indicates a book or document title.
See About the Terminal Server for more information.	This indicates a cross-reference to another chapter or section that you can click on to jump to that section.

Online Help

Online help is provided in the DeviceManager. You can click on the What's This button ( or ) and then click on a field to get field-level help. Or, you can press the **F1** key to get window-level help. You can also get the *User Guide* online by selecting **Help, Help Topics**.

1 Introduction

About the Terminal Server

The Terminal Server is an Ethernet communications/terminal server that allows serial devices to connect directly to LANs. The Terminal Server can connect to a wide range of devices including:

- Terminals for multi-user UNIX systems
- Data acquisition equipment (manufacturing, laboratory, scanners, etc.)
- Retail point-of-sale equipment (bar coding, registers, etc.)
- Modems for remote access and Internet access
- ISDN adapters for branch remote access and Internet access

The performance and flexibility of the Terminal Server allows you to use a wide range of high speed devices in complex application environments. The Terminal Server products will work in any server environment running TCP/UDP/IP.

Terminal Server Models

The Terminal Server comes in several different models to meet your network needs:

- **Terminal Server**—Offered as a 1-port unit (DB25M, DB25F, RJ45, and DB9M interfaces available), this model provides basic Terminal Server functionality and supports software configurable serial interface protocols EIA-232/422/485.
- **Secure Device Server**—This model is available in both desktop and rack mount configurations. Both models support software configurable serial interface protocols EIA-232/422/485. The Secure Device Server model has the advanced secure BLACK BOX[®] feature set in addition to the general Terminal Server functionality.
- **Secure Terminal Server**—This model comes in one desktop model and several rack mount configurations. All models support EIA-232 only. The Secure Terminal Server model has the advanced secure BLACK BOX[®] feature set in addition to the general Terminal Server functionality.
- **Secure Console Server**—This model comes in several rack mount configurations. All models support EIA-232 only and have an internal PCI card interface. The SCS model has the advanced secure BLACK BOX[®] feature set in addition to the general Terminal functionality.

See [Hardware](#) for information about the hardware specifications for your Terminal Server model. See [Software](#) for a list of the basic and advanced software features.

Terminal Server Features

The Terminal Server is a communications server used for making serial network connections. It attaches to your TCP/IP network and allows serial devices such as modems and terminals to access the LAN. It also allows LAN devices to access devices or equipment attached to Terminal Server serial ports. This section highlights the hardware and software components you can expect to find in your Terminal Server model.

Hardware

Hardware Features		BLACK BOX® Models						
		Desktop				Rack Mount		
		Terminal Server	Secure Device Server 1	Secure Device Server 2/4	Secure Terminal Server 4	Secure Device Server	Secure Console Server	Secure Terminal Server
Serial Connectors	DB25F	•	•					
	DB25M	•	•					
	RJ45	•	•	•	•	•	•	•
	DB9M	•	•					
Serial Interface	EIA-232	•	•	•	•	•	•	•
	EIA-422	•	•	•		•		
	EIA-485	•	•	•		•		
Serial Power In Pin	DB25F	•	•					
	DB25M	•	•					
	RJ45	•	•	•	•			
Serial Power Out Pin	DB25F		•					
	DB25M		•					
	RJ45		•	•	•			
Auto Sensing Ethernet Interface	10/100	•	•	•	•			
	10/100/1000					•	•	•
PCI Interface							•	
Power Supply	Power over Ethernet		•	•				
	External AC	•	•	•	•			
	Internal AC					•	•	•
Dedicated Console Port						•	•	•

Software

This section describes the supported software features available.

Accessing the Terminal Server

All Terminal Server models can be accessed through any of the following methods:

- Easy Config Wizard, an easy configuration wizard that allows you to quickly setup the Terminal Server in a Windows® environment
- DeviceManager, a fully functional Windows 2000®/Windows Server 2003®/Windows Server 2003 R2®/Windows XP®/Windows Vista®/Windows Server 2008®/Windows Server 2008 R2®/Windows 7®/Windows 8® and Windows Server 2012® configuration/management tool
- WebManager, a web browser (HTTP/HTTPS) option for configuring/managing the Terminal Server
- Menu, a window-oriented menu interface for configuration and user access
- CLI, a Command Line Interface option for configuration/management and user access
- SNMP, allowing remote configuration via SNMP as well as statistics gathering
- DHCP/BOOTP, a method of automatically updating the Terminal Server

General Features

Basic software features are available on all Terminal Server models.

- IPv6 support.
- Support for TCP/IP and UDP protocols including telnet and raw connections.
- Virtual modem emulation.
- 'Fixed tty' support for several operating systems using the BLACK BOX® COMredirect utility.
- DHCP/BOOTP for automated network-based setup.
- Dynamic statistics and line status information for fast problem diagnosis.
- Modbus master/slave/gateway support.
- Ability to disable services (for example, Telnet, COMredirect, Syslog, SNMP, Modbus, HTTP) for additional security.

Security

The Terminal Server security features can include (depending on your Terminal Server model):

- Supervisory and serial port password protection.
- Ability to set serial port access rights.
- Ability to assign users access level rights to control their access.
- Idle port timers, which close a connection that has not been active for a specified period of time.
- Ability to individually disable network services that won't be used by the Terminal Server.
- Access to fire walled/nated devices via HTTP tunnels.

2 Hardware and Connectivity

Introduction

This chapter describes how to physically set up your Terminal Server unit. It includes an overview of the Terminal Server hardware components and how to power up the Terminal Server to make sure it works correctly.

Terminal Server Components

What's Included

The following components are included with your product:

- Terminal Server unit
- External power supply
- A CD-ROM containing documentation, firmware, configuration software, COMredirect, etc.
- Terminal Server models that have an RJ45 serial connector(s) come with an RJ45→DB9F adapter

What You Need to Supply

Before you can begin, you need to have the following:

- A serial cable(s) to connect serial devices to your Terminal Server unit
- An Ethernet CAT5 10/100/1000BASE-T cable to connect the Terminal Server unit to the network

Power Supply Specifications

Desktop Models

If you are providing a power supply for a desktop Terminal Server model, your power supply must meet the following requirements:

- Output between 9-30V DC.
- DC barrel connector: The cable attached to the power supply should be about 20AWG, length 6 feet approx. The barrel dimensions of the cable-plug are OD=5.5, ID=2.1, and length= 9.5mm, with a straight barrel, and positive polarity on the inside and negative polarity on the outside.
- Power can also be provided by:
 - Serial Port 1, pin 1 on the Terminal Server model.

Getting to Know Your Terminal Server

This section describes the hardware components found on your Terminal Server unit.

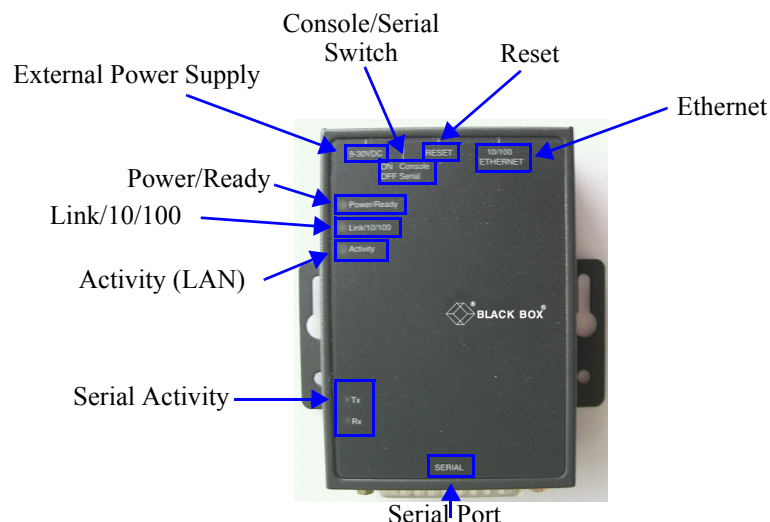
Overview

All Terminal Servers have the same basic hardware components to allow you to connect to serial devices, connect to the network, monitor LAN and serial activity, and manage the unit. Below is a list of these components:

- **Serial Port(s)**—Connector(s) that will be used to connect to a serial device.
- **Activity**—This LED flashes to indicate LAN activity.
- **Link10/100**—This LED indicates the Ethernet connection speed for desktop models:
 - **Green**—10 Mbits
 - **Yellow**—100 Mbits
 - **Off**—no LAN connection
- **Power/Ready**—This LED can cycle through several colors (yellow, green, red) during a boot process, but should complete with a green light. If the LED is green after power up but continues to cycle on and off (flashes green), this indicates that the console switch is in the **on** position. You can learn more about the Power/Ready LED in [Hardware Problems](#).
- **External Power Supply**—This is an external AC power supply.
- **Console/Serial Switch**—This switch determines whether serial port 1 functions as a serial port or a console port.
- **Reset**—The inset RESET button will reboot the Terminal Server if pushed in and released quickly. It will reset the Terminal Server to factory defaults if pushed in and held for more than three seconds. See [Resetting to the Original Factory Default Configuration](#) for more information.
- **Serial Activity**
 - **Tx**—Flashes with transmit serial activity. There is a Tx LED for each serial port.
 - **Rx**—Flashes with receive serial activity. There is an Rx LED for each serial port.
- **Ethernet**—The Ethernet connector.

Terminal Server 1-Port

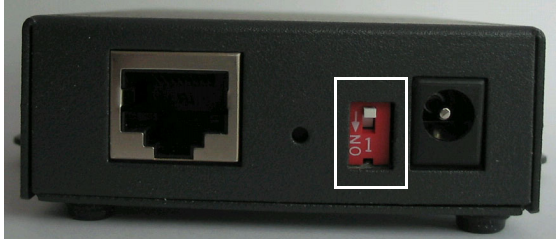
This section describes the components found on the Terminal Server 1-Port model.



The Terminal Server has one serial connection that is one of the following connectors: DB25 male, DB25 female, RJ45, or DB9 male.

Console/Serial Switch

Located at the back of the desktop models is a switch that controls whether serial port 1 is in Console or Serial mode.



Look at your model to verify the direction of the ON switch position. ON indicates that serial port 1 is in Console mode; otherwise serial port 1 is in Serial mode.

Console Mode

Console mode is used when you have a direct connection between a serial device (like a terminal or a PC) and the Terminal Server, accessed by the Admin user to configure/manage the Terminal Server. Console mode automatically sets serial port settings as:

- **Serial Interface** to **EIA-232**
- **Speed** to **9600**
- **Flow Control** to **No**
- **Bits** to **8**
- **Stop Bits** to **1**
- **Parity** to **None**

Console mode also displays extra system messages.

Serial port 1 will ignore any **Serial Port** settings when in Console mode, so you need to turn Console mode off to use serial port 1 in your network.

Note: When the console switch is in the **on** position, the System/Ready LED will blink green.

Serial Mode

Serial mode is used when the Terminal Server acts as a communications server, or anytime you are not connecting directly to the Terminal Server to configure it. You can connect directly to the Terminal Server in Serial mode, but the Terminal Server will not display all the messages/information you will get in Console mode.

Powering Up the Terminal Server

Serial Only Models

To power up the Terminal Server, perform the following steps:

1. Plug the external power supply into the Terminal Server and then into the electrical outlet.
2. You will see the LEDs cycle for several seconds and then remain a solid green, indicating that it is ready to configure/use.

Before you start to configure the Terminal Server, you should set the Terminal Server jumpers if you want to terminate the line or use the power in pin feature (instead of an external power supply, if your desktop Terminal Server model supports it).

In some circumstances, the setting of jumpers may be required:

- Terminal Server models where EIA-422/485 line termination is required.

See [Appendix C, Setting Jumpers](#) to see how to set the jumpers for your Terminal Server desktop model.

3 Configuration Methods

Introduction

This chapter provides information about the different methods you can use to configure the Terminal Server. Before you can configure the Terminal Server, you must assign an IP address to the Terminal Server. See the [Chapter 4, Getting Started](#) to find out how to assign an IP address to the Terminal Server.

Once an IP address is assigned to the Terminal Server, you can use any of the configuration methods to:

- Configure users.
- Configure Terminal Server system parameters.
- Configure serial port parameters.
- Configure network parameters.
- Configure time parameters.
- Reboot the Terminal Server.
- View statistics while connected to the Terminal Server.

Configuration Methods Overview

Some of the Terminal Server configuration methods have the capability of configuring an IP address, which is the first required configuration step for a new Terminal Server. Once the Terminal Server has been assigned an IP address, any of the configuration methods can be used to configure the Terminal Server.

Configures an IP Address

Following is a list of methods for setting the Terminal Server IP address and a short explanation of when you would want to use that method:

- **Easy Config Wizard**—The Easy Config Wizard is available from the CD ROM included with your Terminal Server. You can use the Easy Config Wizard to set the Terminal Server's IP address and configure serial ports. This configuration method would typically be used when:
 - All ports are to have the same configuration.
 - Only the most commonly used profiles are required.
 - Straightforward application with no advanced functionality required. Easy Config is installed on a Windows®-based PC with local network access to the Terminal Server.
- **DeviceManager**—Use this method when you can connect the Terminal Server to the network and access the Terminal Server from a Windows® PC. The DeviceManager is a Windows®-based application that can be used for Terminal Server configuration and management. The DeviceManager can be used to assign an IP address and perform the complete configuration and management of the Terminal Server.

- **Direct Connection**—Use this method when you can connect to the Terminal Server from a serial terminal or from a computer running terminal emulation software over a serial port. Using this method, you will need to configure and/or manage the Terminal Server using either the Menu or CLI.
- **DHCP/BOOTP**—Use this method when you have a BOOTP or DHCP server running and you can connect the Terminal Server to your network. The Terminal Server will automatically obtain an IP address from a local network DHCP/BOOTP server when this service is enabled (it is disabled by default). You can also configure certain Terminal Server parameters that will be passed from the DHCP/BOOTP server to the Terminal Server when it boots up. Other configurators such as DeviceManager, CLI, or Menu can be used to set this option, and obtain the initial IP address.
- **ARP-Ping**—Use this method when you can connect the Terminal Server to the network and want to assign a temporary IP address to the Terminal Server by specifying an ARP entry from your PC and then pinging it.
- **IPv6 Network**—When the Terminal Server is connected to an IPv6 network, its local link address is determined using stateless auto configuration.

Once an IP address has been assigned to the Terminal Server, in most cases, you can continue to use the same method if it is a configurator or you can switch to any other configuration method.

Requires a Configured IP Address

The following configuration methods require that an IP address already be assigned to the Terminal Server.

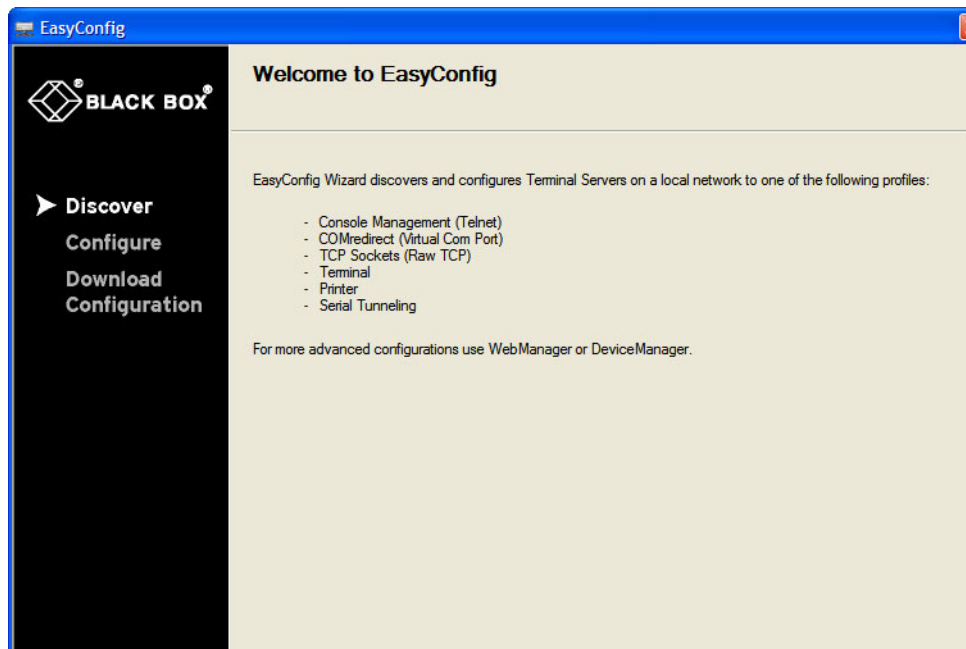
- **WebManager**—WebManager is a fully functional, browser-based configuration method.

Easy Config Wizard

The Easy Config Wizard is a configuration wizard that will configure all the serial ports on your Terminal Server to one of the following:

- Console Management
- COMredirect (Virtual COM Port)
- TCP Sockets (Raw TCP)
- Terminal
- Printer (not supported on Terminal Server 1 Port model)
- Serial Tunneling

You can launch the Easy Config Wizard from the installation CD-ROM.



The Easy Config Wizard has been designed to walk you through the configuration process for any of the available configuration options shown on the Welcome window.

DeviceManager

Overview

The DeviceManager is a Windows®-based application that can be used to connect to the Terminal Server to actively manage and configure it or can create new Terminal Server configurations offline. See [Chapter 5, Using DeviceManager and WebManager](#) for information on configuring/managing the Terminal Server with DeviceManager.

Access Platforms

The DeviceManager can be run from Windows 2000®/Windows Server 2003®/Windows Server 2003 R2®/Windows XP®/Windows Vista®/Windows Server 2008®/Windows Server 2008 R2®/Windows 7®/Windows 8® and Windows Server 2012®. DeviceManager can be installed from the product CD-ROM or downloaded from the Black Box website. Unless the Terminal Server has already been configured with a Gateway, DeviceManager can only access Terminal Servers in the local subnet. Only the admin user can manage or configure the Terminal Server via the DeviceManager.

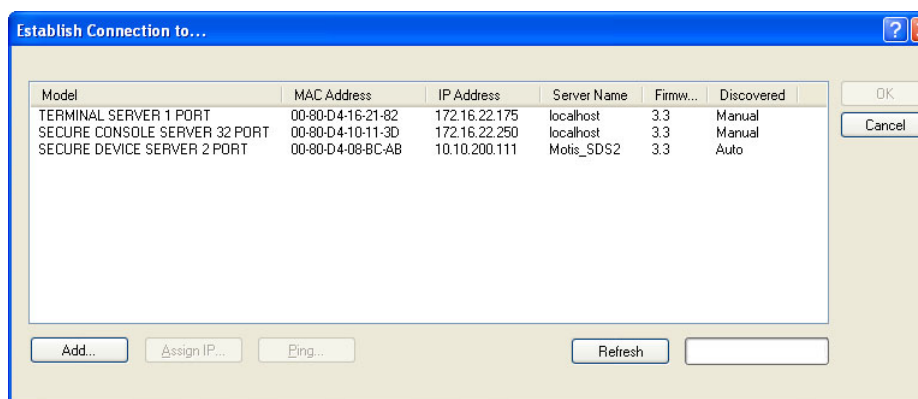
Unique Features

DeviceManager supports the following unique features:

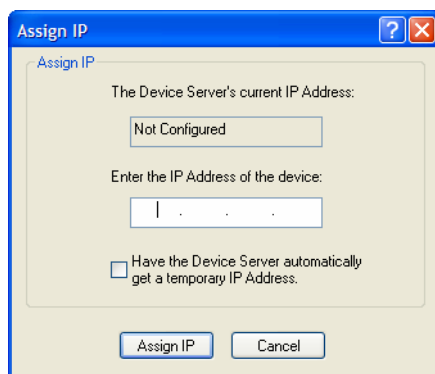
- The ability to download the same configuration file to several Terminal Servers in one operation.
- The ability to save a configuration file locally in text format, in addition to the binary format.
- The ability to create a configuration file without being connected to the Terminal Server.
- The ability to open a session to a Terminal Server and download a (saved) configuration file to it.
- The ability to download custom files, such as new terminal definitions and a custom language files to the Terminal Server.

Connecting to a Terminal Server Using DeviceManager

Before you can use DeviceManager, you need to install it on your Windows operating system from the Terminal Server CD-ROM or you can download it from the Black Box website. After the DeviceManager application is installed, click **Start, All Programs, Black Box, DeviceManager, DeviceManager** to start the application. When you launch the DeviceManager, it will scan the network for Terminal Servers:



All discovered Terminal Server's will be displayed on the list along with their name and IP address. When a new Terminal Server is discovered on the network, that has not yet been assigned an IP address, it will be displayed with an IP Address of **Not Configured**. To configure the IP address, click on the Terminal Server and then click the **Assign IP** button.

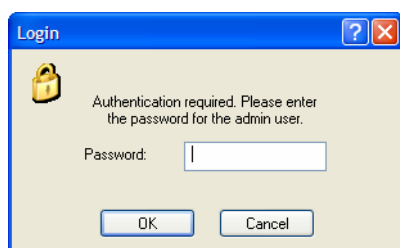


Choose the method you want to use to assign an IP address to the Terminal Server:

- Type in the IP address that you want to assign to this Terminal Server
- Enable the **Have the Terminal Server automatically get a temporary IP Address** option. This will turn on DHCP/BOOTP, so the Terminal Server will attempt to get its IP address from your DHCP/BOOTP server. If you don't have a DHCP/BOOTP server, DeviceManager will temporarily assign an IP address in the range of **169.254.0.1 - 169.254.255.255** that will be used only for the duration of the DeviceManager/Terminal Server communication.

After you configure the IP address, click the **Assign IP** button.

The refreshed list will now display the assigned IP address for the new Terminal Server. To connect to the Terminal Server, click the Terminal Server entry and click **OK**. You will be asked to supply the Admin password (the factory default password is **superuser**).

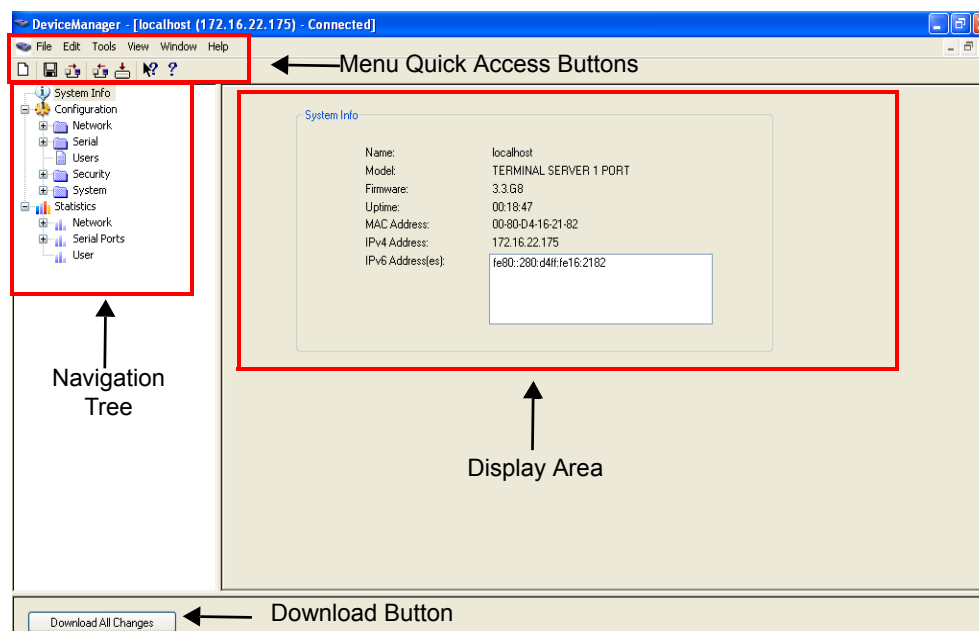


If you have a successful connection, the DeviceManager will retrieve the configuration and then display the Terminal Server's System Information and you can begin configuring the Terminal Server.

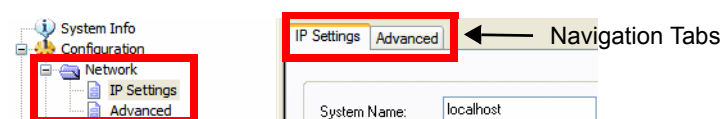
Note: The DeviceManager does not automatically update the Terminal Server's configuration. You must download the configuration changes to the Terminal Server and then reboot the Terminal Server to make the configuration changes take effect

Using DeviceManager

After you have successfully connected to the Terminal Server, you will see the following window:



You navigate through the different configuration windows by selecting an option in the left-hand navigation tree. If double-click on option that is next to a folder, more navigation are displayed when you click on it:



The **Network** folder contains two configuration options, **IP Address** and **Advanced**. Notice that when the **IP Address** option is selected, there are more navigation options in the form of the tabs, **IP Settings** and **Advanced**.

When you have completed all your configuration changes, click the **Download Changes** button to download the configuration to the Terminal Server. You must reboot the Terminal Server to make those configuration changes take effect.

WebManager

Overview

The WebManager is a web-browser based method of configuring/managing the Terminal Server. It follows the same design as the DeviceManager, so it is easy to switch between the WebManager and DeviceManager when configuring your Terminal Server. See [Chapter 5, Using DeviceManager and WebManager](#) for information on configuring/managing the Terminal Server with DeviceManager.

Access Platforms

You can access the Terminal Server through WebManager from any system that can run a web browser. WebManager can be accessed by the admin user or any user who has Admin Level privileges.

Unique Features

WebManager supports the following unique features:

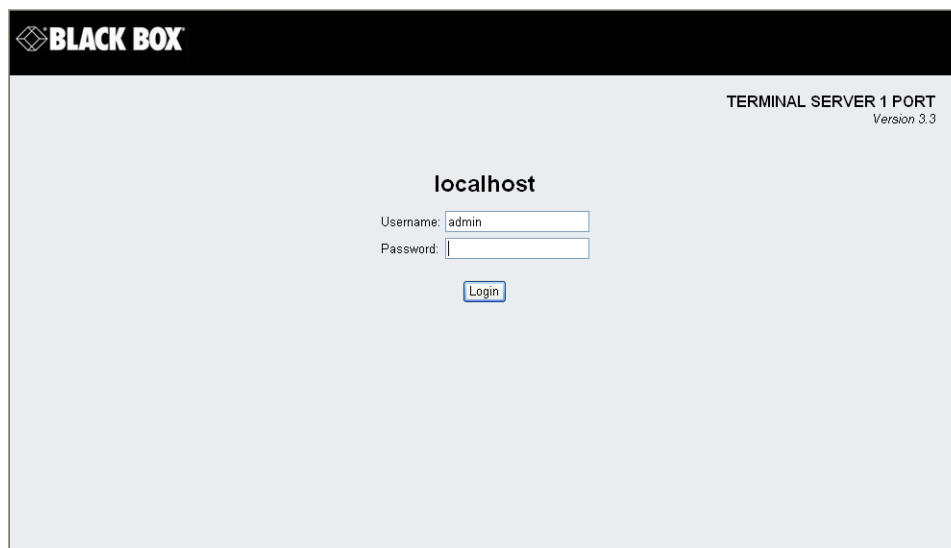
- The ability to open a session to a Terminal Server and download a (saved) configuration file to it.
- The ability to download/upload keys/certificates to/from the Terminal Server.
- The ability to save a configuration file locally in text format, in addition to the binary format.
- The ability to download custom files, such as new terminal definitions and a custom language files to the Terminal Server.

Connecting to a Terminal Server Using WebManager

Before you can connect to a Terminal Server using WebManager, the Terminal Server must already be configured with a known IP address; see [Setting Up the Network](#) to configure an IP address on your Terminal Server.

To connect to the Terminal Server through the WebManager:

1. Open your web browser and type in the IP address of the Terminal Server that you want to manage/configure and press **Enter**; for example: `http://123.123.123.123`.
2. If you successfully connect to the Terminal Server, a login screen will appear.



BLACK BOX

TERMINAL SERVER 1 PORT
Version 3.3

localhost

Username:

Password:

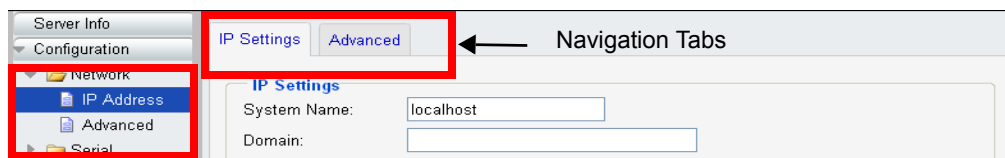
Login

3. If you are accessing the Terminal Server in non-secure HTTP, just type in the Admin password (the factory default password is **superuser**) Using WebManager

After you have successfully logged into WebManager, you will see the following:



You navigate through the different configuration windows by selecting an option in the left-hand navigation tree. If click on option that is next to a folder, more navigation are displayed when you click on it:



The **Network** folder contains two configuration options, **IP Address** and **Advanced**. Notice that when the **IP Address** option is selected, there are more navigation options in the form of the tabs, **IP Settings** and **Advanced**.

Remember that in the WebManager, it is necessary to press the **Apply** button to save your changes.

Command Line Interface

Overview

The Command Line Interface (CLI) is a command line option for Terminal Server configuration/management. See the *Command Line Interface Reference Guide* for a full breakdown of all the CLI commands and their functionality.

Access Platforms

The CLI is accessed by any application that supports a Telnet session to the Terminal Server's IP address, such as Putty, SecureCRT, or from a command prompt. You can also access the CLI from a dumb terminal or PC connected to a serial port.

Unique Features

The CLI supports the following unique features:

- You can access a Terminal Server from any application that supports Telnet.T
- The ability to save a configuration file locally in text format, in addition to the binary format.
- Ability to clear the ARP table (cache).

Connecting to a Terminal Server Using the CLI

There are two ways you can access the Terminal Server, through the network (Ethernet connection) or through the serial connection. If you are accessing the Terminal Server through the network, the Terminal Server must already have a known IP address configured; see [Using a Direct Serial Connection to Specify an IP Address](#) getting started for information on configuring an IP address.

Through the Network

To connect to the Terminal Server through the network to configure/manage it using the CLI, do the following:

1. Start a Telnet session to the Terminal Server's IP address; for example:

```
telnet 10.10.201.100
```

2. You will get a **Login:** prompt. You can login as the admin user or as a user with Admin Level rights. If the login is successful, you will get a prompt that displays the Terminal Server model and number of ports:

```
Login: admin
Password:
```

```
Terminal Server 1 Port#
```

You will see a prompt that displays the Terminal Server model name and number of serial ports. You are now ready to start configuring/managing your Terminal Server using the CLI.

Through the Serial Port

To connect to the Terminal Server through the serial port to configure/manage it using the CLI (or Menu), see [Using a Direct Serial Connection to Specify an IP Address](#).

After you have established a connection to the Terminal Server, you will get a **Login:** prompt. You can login as the admin user or as a user with Admin Level rights. If the login is successful, you will get a prompt that displays the Terminal Server model and number of ports:

```
Login: admin
Password:
```

```
Terminal Server 1 Port#
```

You will see a prompt that displays the Terminal Server model name and number of serial ports. You are now ready to start configuring/managing your Terminal Server using the CLI

Using the CLI

After you have successfully logged in, you can start configuring/managing the Terminal Server by typing in commands at the prompt. If you are not sure what commands are available, you can type a? (question mark) at any time during a command to see your options.

See the *Command Line Interface Reference Guide* for more information about the CLI.

Menu

Overview

The Menu is a graphical representation of the CLI. You can look up Menu parameter explanations in the *Command Line Interface Reference Guide*. The only operations that the Menu does not support are the downloading and uploading of files to/from the Terminal Server.

Access Platforms

The Menu is accessed by any application that supports a Telnet session to the Terminal Server's IP address, such as Putty, SecureCRT, or from a command prompt. You can also access the Menu from a dumb terminal or PC connected to a serial port.

Unique Features

The Menu supports the following unique feature:

- You can access a Terminal Server from any application that supports Telnet.
- You can access the Terminal Server using a terminal emulator and a serial connection.

Connecting to the Terminal Server Using the Menu

To connect the Terminal Server using the Menu, follow the directions for [Connecting to a Terminal Server Using the CLI](#).

Using the Menu

After you have successfully logged in, type **screen** at the prompt and press **Enter**. You will be asked to enter a terminal type, and then you will see the following Menu:



To navigate through the Menu options, do the following:

1. Highlight a Menu option by using the keyboard up and down arrows to navigate the list.
2. When the Menu item you want to access is highlighted, press the **Enter** key to either get to the next list of options or to get the configuration screen, depending on what you select.
3. When you are done configuring parameters in a screen, press the **Enter** key and then the **Enter** key again to **Accept and exit the form**.
4. If you want to discard your changes, press the **Esc** key to exit a screen, at which point you will be prompted with **Changes will be lost, proceed? (y/n)**, type **y** to discard your changes or **n** to return to the screen so you can press **Enter** to submit your changes.

5. If there are a number of predefined options available for a field, you can scroll through those items by pressing the **Space Bar** or you can type **1** (lowercase L) to get a list of options, use the up/down arrows to highlight the option you want, and then press **Enter** to select it.

DHCP/BOOTP

Overview

Several Terminal Server parameters can be configured through a DHCP/BOOTP server during the Terminal Server bootup. This is particularly useful for configuring multiple Terminal Servers.

Not all configuration parameters are supported in the DHCP/BOOTP configuration (see [DHCP/BOOTP Parameters](#) for supported configuration parameters), so you will need to use another configuration method, such as DeviceManager, WebManager or CLI, to complete the configuration.

Unique Features

DHCP/BOOTP supports the following unique features:

- DHCP/BOOTP can supply the Terminal Server's IP address.
- The DHCP/BOOTP server can configure certain server and user configuration parameters when the Terminal Server is booted.
- The DHCP/BOOTP server can auto-configure the Terminal Server with basic setup information (IP address, subnet/prefix bits, etc.).
- The DHCP/BOOTP server can download a new version of firmware when a Terminal Server is rebooted.
- The DHCP/BOOTP server can download a full configuration file when a Terminal Server is rebooted.

Connecting to the Terminal Server Using DHCP/BOOTP

The Terminal Server will automatically request an IP address from the DHCP/BOOTP server when the **Obtain IP address automatically using DHCP/BOOTP** parameter is enabled. To enable the **Obtain IP address automatically using DHCP/BOOTP** parameter, follow the directions in [Using a Direct Serial Connection to Enable BOOTP/DHCP](#).

Using DHCP/BOOTP

To use DHCP/BOOTP, edit the bootp file with Terminal Server configuration parameters. You can use DHCP/BOOTP to perform the following actions on a single or multiple Terminal Servers on bootup:

- auto-configure with minimal information; for example, only an IP address
- auto-configure with basic setup information (IP address, subnet/prefix bits, etc.)
- download a new version of firmware
- download a full configuration file

DHCP/BOOTP is particularly useful for multiple installations: you can do all the Terminal Server's configuration in one DHCP/BOOTP file, rather than configure each Terminal Server manually. Another advantage of DHCP/BOOTP is that you can connect a Terminal Server to the network, turn on its power and let autoconfiguration take place. All the configuration is carried out for you during the DHCP/BOOTP process.

DHCP/BOOTP Parameters

The following parameters can be set in the DHCP/BOOTP bootp file:

- **SW_FILE**—The full path, pre-fixed by hostname/IP address (IPv4 or IPv6), and file name of the firmware update.
- **CONFIG_FILE**—The full path, pre-fixed by hostname/IP address (IPv4 or IPv6), and file name of the configuration file. Note: these parameters include clear text user passwords.
- **GUI_ACCESS**—Access to the Terminal Server from the HTTP WebManager. Values are **on** or **off**.
- **SECURITY**—Restricts Terminal Server access to devices listed in the Terminal Server's host table. Values are **yes** or **no**.
- **TFTP_RETRY**—The number of TFTP attempts before aborting. This is a numeric value, for example, 5.
- **TFTP_TMOUT**—The time, in seconds, before retrying a TFTP download/upload. This is a numeric value, for example, 3.
- **CUSTOM_LANG**—The full path, pre-fixed by a hostname/IP address (IPv4 or IPv6), and file name of a translated language file. For example,
192.101.34.211 /accounting/bb_ds_german.txt.
- **EXTRA_TERM1**—(**EXTRA_TERM2**, **EXTRA_TERM3**) The full path, pre-fixed by a hostname/IP address (IPv4 or IPv6), and file name of a termcap file for a specific terminal type.

SNMP

Overview

The Terminal Server supports configuration and management through SNMP. SNMP Management tools (SNMP client/MIB browser software) can be used to set Terminal Server configuration parameters and/or view Terminal Server statistics.

Before you can configure/manage the Terminal Server using SNMP, although you need to set the Terminal Server IP address and configure a read-write user for SNMP version 3 or a community for SNMP version 1 or 2. You can use DeviceManager, CLI, or the Menu to set the IP address and user/community (don't forget to reboot the Terminal Server before connecting with the SNMP manager to make your changes take effect).

Access Platforms

You can access the Terminal Server SNMP MIB from any system that runs your SNMP client/MIB browser software.

Unique Features

SNMP supports the following unique features:

- You can configure SNMP traps.
- Since not all versions of SNMP support secure communication, password parameters must be set using another configuration method.

Connecting to the Terminal Server Using SNMP

Before you can connect to the Terminal Server through an SNMP Management tool or MIB browser, you need to set the following components through another configuration method.

1. Configure a known IP address on the Terminal Server.
2. Configure a read-write user for SNMP version 3 or a community for SNMP version 1 or 2 on the Terminal Server.
3. Reboot the Terminal Server to make sure the changes take effect.

To connect to the Terminal Server through an SNMP Management tool or MIB browser, do the following:

1. Load the **blackbox-ds.MIB** file from the Terminal Server CD-ROM into your SNMP manager.

Note: You need to have the following MIBs installed in your SNMP manager (these are usually part of the standard SNMP client/MIB browser):

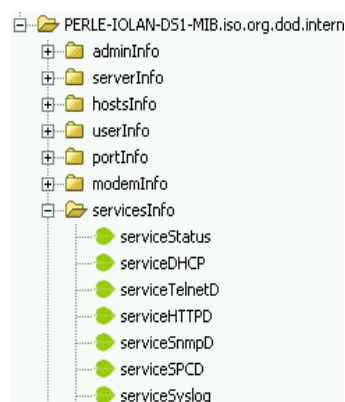
- SNMPv2-SMI
- SNMPv2-TC
- IPV6-TC

2. Verify that the read-write user for SNMP version 3 or a community for SNMP version 1 or 2 match the configuration on the Terminal Server.
3. Type in the Terminal Server's IP address and connect to the Terminal Server.

You are now ready to start configuring the Terminal Server using SNMP.

Using the SNMP MIB

After you have successfully connected to the Terminal Server through your SNMP Management tool or MIB browser, expand the **BLACKBOX-Terminal-Server-MIB** folder to see the Terminal Server's parameter folders. Below is an example of the configurable parameters under the **servicesinfo** folder.



The first variable in each folder is the **Status** variable, for example, **serviceStatus**. When you perform a **GET** on this variable, one of the following values will be returned:

- **1**—Indicates that the container folder is active with no changes.
- **2**—Indicates that the container folder is active with change(s).

Once you have completed setting the variables in a folder, you will want to submit your changes to the Terminal Server. To do this, set the **Status** variable to **4**. If you want to discard the changes, set the **Status** variable to **6**.

- **4**—Indicates that the changes in the container folder are to be submitted to the Terminal Server.
- **6**—Indicates that the changes in the container folder are to be discarded.

If you want to save all the changes that have been submitted to the Terminal Server, you need to expand the **adminInfo** container folder and **SET** the **adminFunction** to **1** to write to FLASH. To make the configuration changes take effect, **SET** the **adminFunction** to **3** to reboot the Terminal Server

4 Getting Started

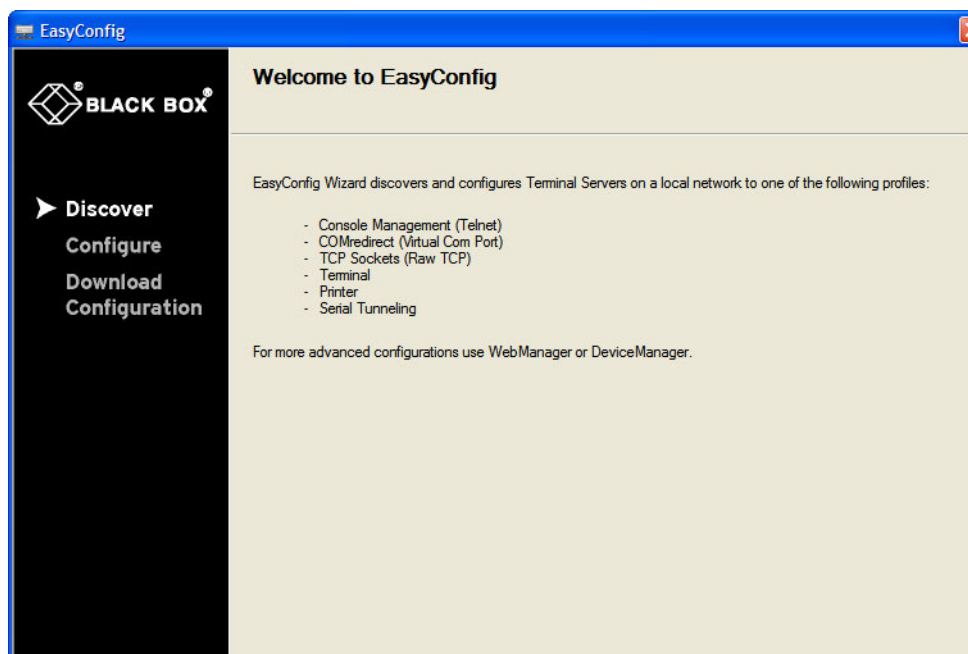
Introduction

There are several different configuration methods available to configure the Terminal Server (see [Chapter 3, Configuration Methods](#) for more information). This chapter describes the three main minimal configuration requirements for the Terminal Server through either Easy Config Wizard (cannot configure users using this method), DeviceManager, or WebManager:

1. **Setting up the network**—This minimally consists of configuring an IP address or enabling DHCP/BOOTP. Once the Terminal Server has an IP address, you can use any configuration method.
2. **Setting up the serial ports**—You will want to select the serial port profile that matches the serial port requirement/scenario for your serial device.
3. **Setting up users**—This is an optional step, which is only required when your implementation requires users to access the Terminal Server.

Easy Configuration Wizard

The Easy Config Wizard quickly sets up the Terminal Server's network configuration and all serial ports to one of the following:



- **Console Management**—Allows users on the network to connect to a serial device that is connected to a serial port on the Terminal Server.

- **COMredirect (Virtual COM Port)**—Allows a networked system to communicate with your serial device through a virtual COM or TTY port, using the Black Box COMredirect software.
- **TCP Sockets (Raw TCP)**—Allows hosts on the network to communicate with a serial device that requires raw data throughput (such as a printer or card reader) connected to the Terminal Server serial port.
- **Terminal**—Allows a terminal device to connect to a specified host on the network through a serial port on the Terminal Server.
- **Printer**—(Not supported on Terminal Server 1-Port model) Allows hosts on the network to talk to a printer using LPD or RCP connected to the Terminal Server.
- **Serial Tunneling**—Allows Terminal Servers on the network to establish a virtual link between their serial ports. Typically, one Terminal Server's serial port is configured as a Tunnel Server and the other Terminal Server's serial port is configured as a Tunnel Client.

Setting Up the Network

The most important part of setting up the network is assigning an IP address to the Terminal Server, whether this is a static IP address or enabling a DHCP/BOOTP-assigned IP address. You should also assign a name to the Terminal Server, to make it easier to recognize. This section deals primarily with setting the IP address.

Using DeviceManager

To use the DeviceManager, you must first install it on a Windows® operating system. The DeviceManager is able to automatically discover all Terminal Servers on your local network, even if they have not yet been assigned an IP address. If routers on the network have been setup to propagate multicasts, DeviceManager will also be able to discover Terminal Servers in other networks. The DeviceManager installation wizard can be found on the CD-ROM included in the Terminal Server package.

1. Connect the Terminal Server to the network.
2. Power on the Terminal Server.
3. From the CD-ROM that was included in the Terminal Server packaging, select the DeviceManager link.
4. Click on the link under **Location** and click **Open** to automatically start the DeviceManager installation.
5. Install the DeviceManager by following the installation wizard. On the last window, check the **Yes, I want to launch DeviceManager now.** box and click the **Finish** button.
6. When you launch the DeviceManager, it will automatically scan the local network and display any Terminal Servers that it can find.
7. Any Terminal Server that does not have an IP address will be displayed as **Not Configured**, with the **Model** and **MAC Address** to identify the Terminal Server. Highlight the Terminal Server that you want to assign an IP address to and click the **Assign IP** button.
8. Choose the method you want to use to assign an IP address to the Terminal Server:
 - Type in the IP address that you want to assign to this Terminal Server.
 - Enable the **Have the Terminal Server automatically get a temporary IP address** option. This will turn on DHCP/BOOTP, so the Terminal Server will attempt to get its IP address from your DHCP/BOOTP server. If you don't have a DHCP/BOOTP server, DeviceManager will temporarily assign an IP address in the range of **169.254.0.1 - 169.254.255.255** that will be used only for the duration of the DeviceManager/Terminal Server communication.

Click the **Assign IP** button.

9. You are now ready to configure the Terminal Server. Double-click the Terminal Server you just configured the IP address for to open a configuration session. Type **superuser** (the factory default Admin user password) in the Login window and click **OK**.
10. Expand the **Server Configuration** folder and select **Server**. Verify the IP address configuration. You should also enter a name in the **Server Name** field to make the Terminal Server easily identifiable.
11. To make your edits take effect, you need to download the new configuration file and then reboot the Terminal Server. Download the configuration file to the Terminal Server by selecting **Tools, Download Configuration to Unit** or click the **Download All Changes** button.
12. Reboot the Terminal Server by selecting **Tools, Reboot Server** or click the **Reboot** Terminal Server button.

For more information on configuring the Terminal Server using DeviceManager, see [Chapter 5, Using DeviceManager and WebManager](#).

Using WebManager

To use the WebManager as your configurator, you must first assign an IP address to the Terminal Server. You can use the Easy Config Wizard to assign an IP address to the Terminal Server or any of the other methods described in this section. Once the IP address is assigned to the Terminal Server, simply type the IP address into the **Address** field of your web browser and press the **Enter** key.

Using a Direct Serial Connection to Specify an IP Address

You can connect to the Terminal Server's serial console port using a PC with a terminal emulation package, such as HyperTerminal or a terminal.

1. Connect the Terminal Server to your PC or dumb terminal. Make sure the DIP switch is in Console mode (desktop models, this sets the Terminal Server serial port 1 to EIA-232). When connecting a terminal or PC directly (without modems), the EIA-232 signals need to be crossed over ('null modem' cable). For RJ45 models, the RJ45 to DB9F adaptor shipped with the unit will provide this crossover.
2. Using a PC emulation application, such as HyperTerminal, or from a dumb terminal, set the Port settings to 9600 Baud, 8 Data bits, No Parity, 1 Stop Bits, and No Hardware Flow control to connect to the Terminal Server.
3. When prompted, type **admin** for the User and **superuser** for the Password. You should now see the a prompt that displays the model type and port number; for example, **Terminal Server 1 port#**.
4. You are now logged into the Terminal Server and can set the IP address by typing from the command line using the Command Line Interface (CLI).

Type:

```
set server internet <ipv4address>
```

Where **ipv4address** is the IP Address being assigned to the Terminal Server.

5. Type the following command:

```
save
```

6. If you are going to use another configuration method, such as WebManager or DeviceManager, the Terminal Server will need to be re-booted first. On a desktop unit, change the DIP switch to the OFF (Serial) position before re-booting the Terminal Server. Plug the Terminal Server back in, automatically rebooting the Terminal Server in the process.

7. If you want to complete the configuration using a direct connection, see [Command Line Interface](#) and/or [Menu](#) . After you complete configuring the Terminal Server, it will need to be re-booted for the configuration to take effect. On a desktop unit, change the DIP switch to the OFF (Serial) position before re-booting the Terminal Server. Plug the Terminal Server back in, automatically rebooting the Terminal Server in the process.

Using a Direct Serial Connection to Enable BOOTP/DHCP

If you are using BOOTP, you need to add an entry in the BOOTP server for the Terminal Server that associates the MAC address (found on the back of the Terminal Server) and the IP address that you want to assign to the Terminal Server. After you have made the MAC address/IP address association for BOOTP, use the following directions for BOOTP or DHCP.

You can connect to the Terminal Server using a PC with a terminal emulation package, such as HyperTerminal or a dumb terminal.

1. Connect the Terminal Server to your PC or dumb terminal. Make sure the DIP switch is in Console mode (desktop models, this sets the Terminal Server serial port to EIA-232). When connecting a terminal or PC directly (without modems), the EIA-232 signals need to be crossed over ('null modem' cable). For RJ45 models, the RJ45 to DB9F adaptor shipped with the unit will provide this crossover.
2. Using a PC emulation application, such as HyperTerminal, or from a dumb terminal, set the Port settings to 9600 Baud, 8 Data bits, No Parity, 1 Stop Bits, and No Hardware Flow control to connect to the Terminal Server.
3. When prompted, type **admin** for the User and **superuser** for the Password. You should now see the a prompt that displays the model type and port number; for example, **Terminal Server 1 port#**.
4. You are now logged into the Terminal Server and can set the IP address by typing from the command line using the Command Line Interface (CLI). Type the following command:

```
set server internet dhcp/bootp on
```
5. Type the following command:

```
save
```
6. Type the following command:

```
reboot
```
7. When the Terminal Server reboots, it will automatically poll for an IP address from the DHCP/BOOTP server. If you have a Terminal Server with dual Ethernet, each Ethernet connection will automatically be assigned an IP address, you can access the Terminal Server through either IP address.
8. To view the DHCP/BOOTP assigned IP address, type the following command:

```
show interface ethernet
```

If for some reason it cannot obtain an IP address from your DHCP/BOOTP server, you will have to either reconnect to the Terminal Server on the console port and reboot it or push the Reset to Factory button to access the Terminal Server.

You are now ready to configure the Terminal Server. See [Chapter 3, Configuration Methods](#) for information on the different Terminal Server configuration methods.

Using ARP-Ping

You can use the ARP-Ping (Address Resolution Protocol) method to temporarily assign an IP address and connect to your Terminal Server to assign a permanent IP address. To use ARP-Ping to temporarily assign an IP address:

1. From a local UNIX/Linux host, type the following at the system command shell prompt:

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

On a Windows[®] 2000 or newer system, type the following at the command prompt:

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

(where **a.b.c.d** is the IPv4 address you want to temporarily assign to the Terminal Server, and **aa:bb:cc:dd:ee:ff** is the Ethernet (MAC) address of Terminal Server (found on the back of the unit).

2. Whether you use UNIX or Windows[®], you are now ready to ping to the Terminal Server. Here is a UNIX example of the sequence to use:

```
arp -s 192.168.209.8 00:80:d4:00:33:4e
ping 192.168.209.8
```

From the ping command issued in step 2, the Terminal Server will pickup and use the IP address entered into the ARP table in step 1. You are now ready to configure the Terminal Server. See [Chapter 3, Configuration Methods](#) for information on the different Terminal Server configuration methods.

For an IPv6 Network

The Terminal Server has a factory default link local IPv6 address that takes the following format:

Terminal Server MAC Address: 00-80-D4-AB-CD-EF

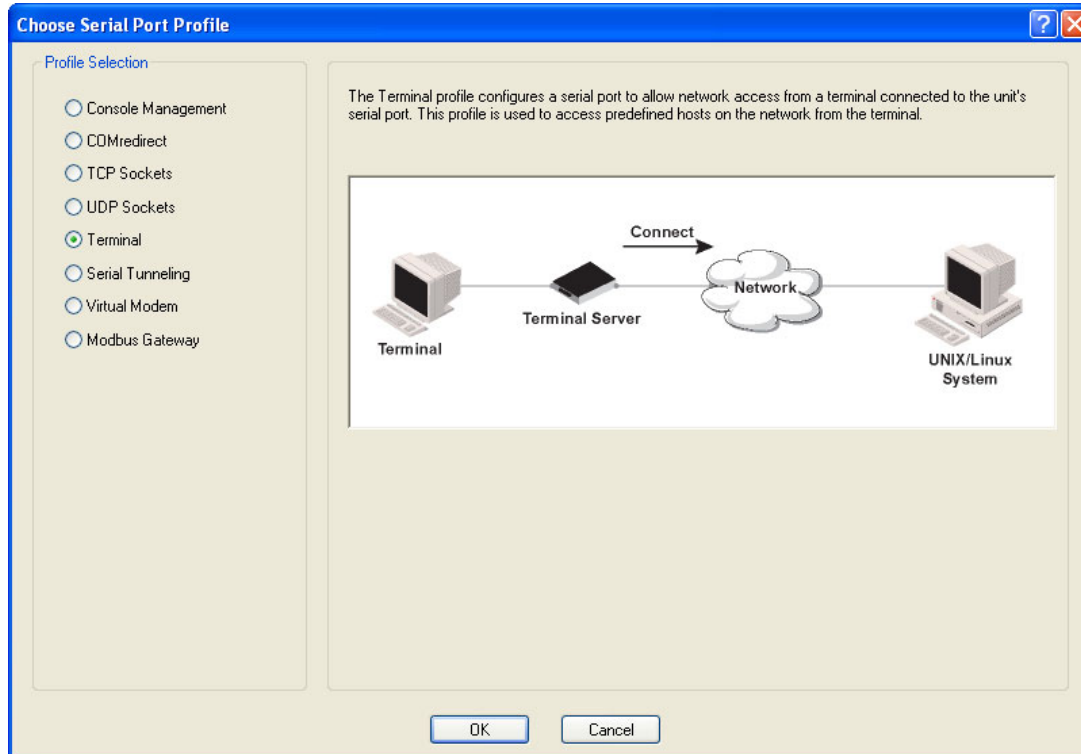
Link Local Address: fe80::0280:D4ff:feAB:CDEF

The Terminal Server will also listen for IPv6 router advertisements to learn a global address. You do not need to configure an IPv4 address for a Terminal Server residing in an IPv6 network.

You are now ready to configure the Terminal Server. See [Chapter 3, Configuration Methods](#) for information on the different Terminal Server configuration methods.

Setting Up the Serial Port(s)

The DeviceManager and WebManager have the following serial port profiles that will simplify serial port setup:

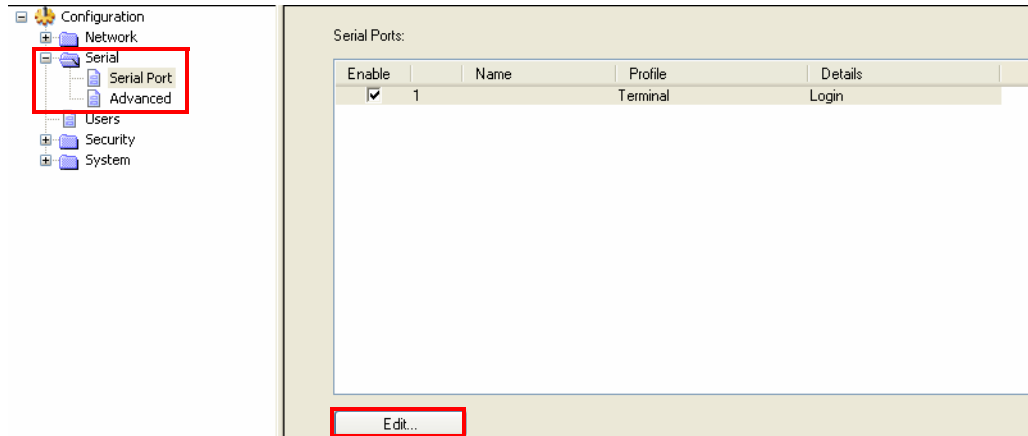


- **Console Management**—The Console Management profile configures a serial port to provide network access to a console or administrative port. This profile sets up a serial port to support a TCP socket that listens for a Telnet connection from the network.
- **COMredirect**—The COMredirect profile configures a serial port to connect network servers or workstations running the COMredirect software to a serial device as a virtual COM port. This profile is ideal for connecting multiple serial ports to a network system or server.
- **TCP Sockets**—The TCP Sockets profile configures a serial port to allow a serial device to communicate over a TCP network. The TCP connection can be configured to be initiated from the network, a serial device connected to the serial port, or both. This is sometimes referred to as a raw connection or a TCP raw connection.
- **UDP Sockets**—The UDP Sockets profile configures a serial port to allow communication between the network and serial devices connected to the Terminal Server using the UDP protocol.
- **Terminal**—The Terminal profile configures a serial port to allow network access from a terminal connected to the Terminal Server's serial port. This profile is used to access predefined hosts on the network from the terminal.
- **Serial Tunneling**—The Serial Tunneling profile configures a serial port to establish a virtual link over the network to a serial port on another Terminal Server. Both Terminal Server serial ports must be configured for Serial Tunneling (typically one serial port is configured as a Tunnel Server and the other serial port as a Tunnel Client).
- **Virtual Modem**—The Virtual Modem (Vmodem) profile configures a serial port to simulate a modem. When the serial device connected to the Terminal Server initiates a modem connection, the Terminal Server starts up a TCP connection to another Terminal Server configured with a Virtual Modem serial port or to a host running a TCP application.

- **Modbus Gateway**—The Modbus Gateway profile configures a serial port to act as a Modbus Master Gateway or a Modbus Slave Gateway.

Each serial port profile contains all the parameters that are required to completely configure the serial port scenario represented by the profile.

To select a serial port profile in the DeviceManager, connect through the DeviceManager to the Terminal Server you are configuring and select **Serial, Serial Ports** in the navigation pane. Highlight the serial port you want to configure and then click **Edit**.

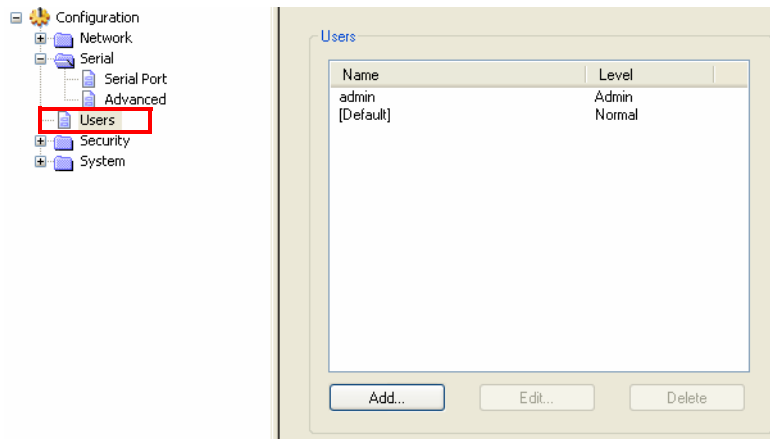


When the default serial port profile Terminal displays, click the **Change Profile** button and select the appropriate profile for the serial port. See [Chapter 6, Configuring Serial Ports](#) for more information on the serial port profiles and their configuration parameters.

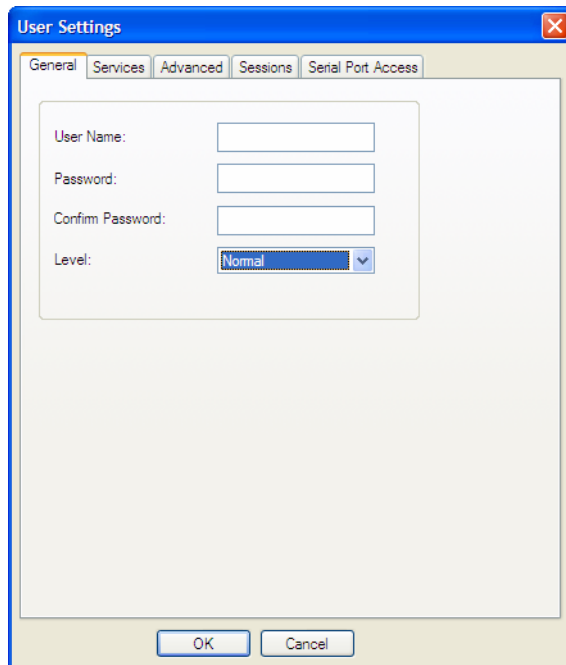
Setting Up Users

When you have a user who is accessing a device connected to a serial port from the network or who is accessing the network from a device connected to a serial port through the Terminal Server, you can create a user account and configure the user's access privileges. Notice that there is a Default user; the Default user's parameters are inherited by users accessing a serial port configured for the **Terminal** profile with the **Connect to remote system** option enabled.

To add a user account, click on the **Users** page in the navigation pane.



Click the **Add** button to create a user account.



To quickly add a user, fill out the field in the **General** tab and click **OK**.

See [Chapter 8, Configuring Users](#) for more information about the other user parameters you can configure.

5

Using DeviceManager and WebManager

Introduction

The DeviceManager and WebManager Terminal Server managers have been designed to be very similar to use. DeviceManager is a Windows®-based application and WebManager is a browser-based application. Both options use the Terminal Server's IP address to access the Terminal Server; the DeviceManager can be used to assign an IP address to a new Terminal Server and the WebManager requires that the Terminal Server already have an IP address before it can be used to configure the Terminal Server.

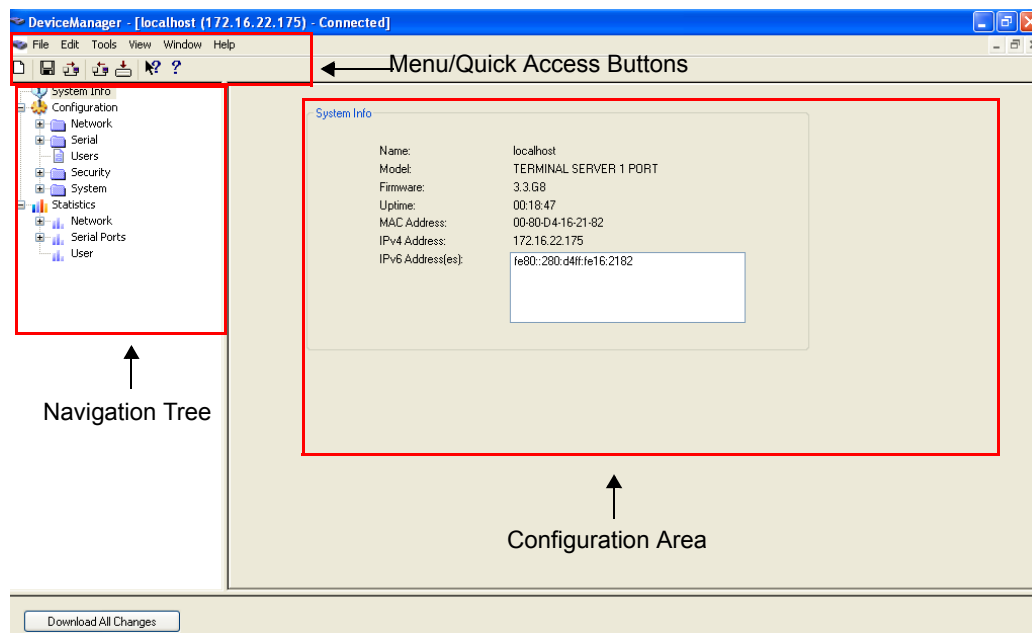
When using WebManager, you are required to click the **Apply** button each time you make a change to a configuration window/tab. In DeviceManager, you must download your configuration changes to the Terminal Server either periodically or after you are done with the configuration changes. From both managers you must reboot the Terminal Server in order for your configuration changes to take effect.

Navigating DeviceManager/WebManager

The DeviceManager and WebManager have very similar navigation methods. The left-hand side of the manager is the navigation tree and the center is the configuration area. The DeviceManager has menu and quick access buttons, whereas the WebManager has system information and some navigation options on the far right-hand side.

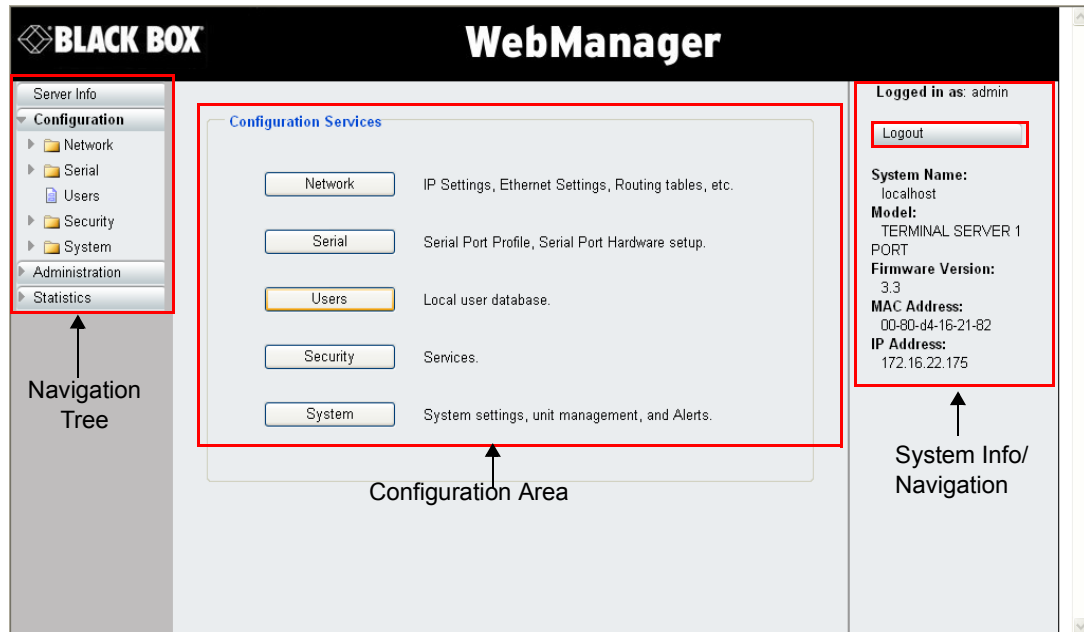
DeviceManager

The DeviceManager uses a folder/page navigation tree. You can expand the folders to see the available configuration pages. When you access a configuration page, you can often navigate the tabs in the configuration area to access all of the configuration options.



WebManager

The WebManager uses an expandable/collapsible buttons with folders and pages for the navigation tree. You can expand the buttons to view the folders and pages to see the available configuration options. When you access a configuration page, you can often navigate the tabs in the configuration area to access all of the configuration options.



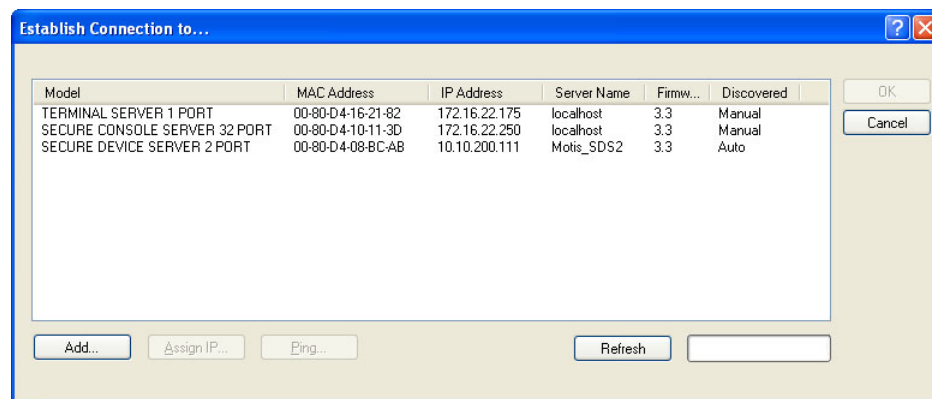
Using DeviceManager to Connect to the Terminal Server

DeviceManager can connect to existing Terminal Servers or assign an IP address to a new Terminal Server. Whenever you connect to a Terminal Server through the DeviceManager, you connect as the Admin user and must supply the password for the Admin user.

Starting a New Session

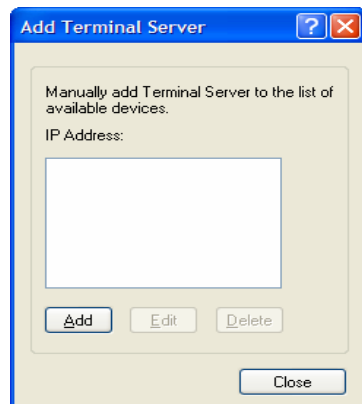
To start a new session and connect to the Terminal Server using the DeviceManager:

1. Start the DeviceManager by selecting **Start, All Programs, Black Box, DeviceManager, DeviceManager**.
2. When the DeviceManager starts, it searches the network for Terminal Servers.



Note: If you are not seeing IPv6 addresses in the list (you must expand the entry), see [IPv6 Issues](#) to find out how to install IPv6 support.

If your Terminal Server is not in the local network and you do not have a multicast enabled router in your network and therefore is not displayed in the selectable list, but can be pinged from your PC, you can add it to the selectable list by clicking the **Add** button.

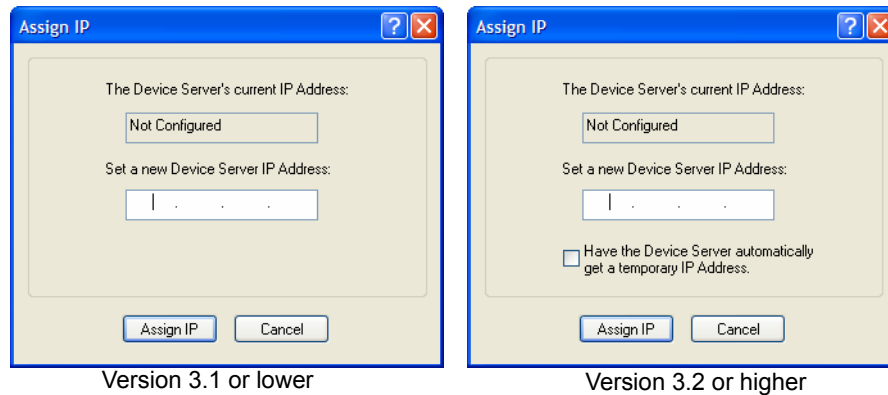


Click the **Add** button and type in the Terminal Server's IP address; this field supports IPv4 and IPv6 addresses. Click the **Close** button when you have completed adding all the manual entries. Select the manually added server to connect to it.

Assigning a Temporary IP Address to a New Terminal Server

You can temporarily assign an IP address to a Terminal Server that is connected to your local network segment, for the purpose of connecting to it and downloading a configuration file (containing a permanent IP address). To temporarily assign an IP address to a Terminal Server, do the following:

1. Click the **Refresh** button. The Terminal Server will be displayed in the **IP Address** column as **Not Configured**.
2. Select the new Terminal Server and click the **Assign IP** button. The following window is displayed:

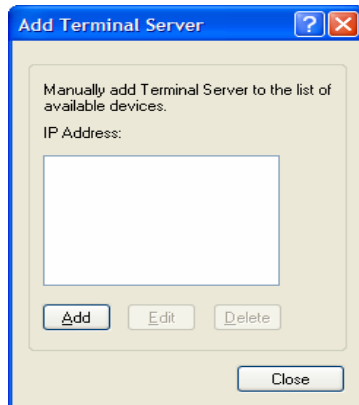


3. Type a valid temporary IP address into the address field or, in version 3.2 or higher, enable the **Have the Terminal Server automatically get a temporary IP address**. If you enable the temporary IP address, the Terminal Server will enable DHCP/BOOTP on your Terminal Server and attempt to get an IP address from the DHCP/BOOTP server (this will permanently enable DHCP/BOOTP in your Terminal Server's configuration, until you change it). If your network does not have a DHCP/BOOTP server, the Terminal Server will temporarily assign an IP address in the range of **169.254.0.1 - 169.254.255.255** (this IP address is only assigned for the duration of the Terminal Server connection).
4. Click the **Assign IP** button.
5. Double-click the Terminal Server in the Terminal Server **List**. If this is the first time you are accessing the Terminal Server, type in the factory default Admin password, **superuser**, and click **OK**. The DeviceManager will display a window indicating that it is trying to authenticate and connect you on the Terminal Server.
6. If the authentication and connection are successful, the Server Info window is displayed. You are now ready to configure the Terminal Server. If authentication was unsuccessful, try to connect to the Terminal Server again; you probably mistyped the password for the Admin user.

For more information about managing a Terminal Server, see [Configuration Files](#).

Adding/Deleting Manual Terminal Servers

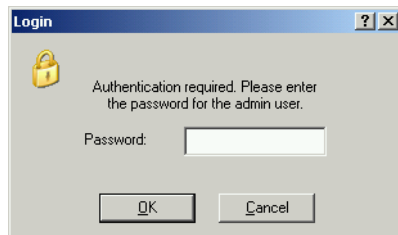
To permanently add or delete a Terminal Server to/from the Terminal Server **List**, click the **Add** button. The following window is displayed:



To permanently add the Terminal Server to the Terminal Server list, type in the IP address of the Terminal Server and click the **Add** button and enter the IPv4 or IPv6 address. To permanently delete the Terminal Server from the Terminal Server list, select the Terminal Server's IP address and click the **Delete** button.

Logging in to the Terminal Server

To log in to a Terminal Server, double-click on the Terminal Server in the **Device Server List**. You will be prompted for the Admin Password (the default is **superuser**).



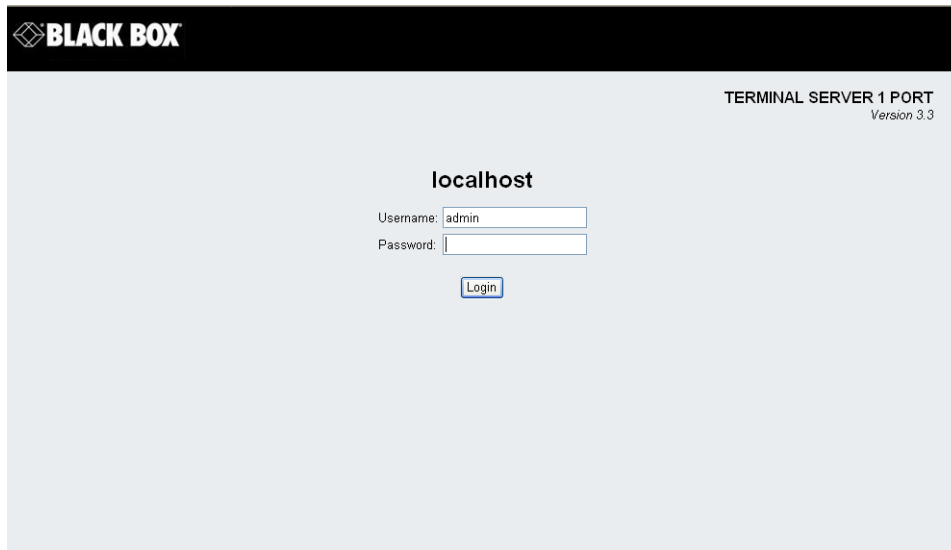
If the authentication and connection are successful, the Terminal Server's **Server Info** window is displayed.

If you cannot connect to a Terminal Server, you can highlight the Terminal Server and click the **Ping** button to verify that the DeviceManager can communicate with the Terminal Server's IP Address. If the ping times out, then you might need to set up a Gateway in your Terminal Server or verify that your network is communicating correctly.

Using WebManager to Connect to the Terminal Server

WebManager can only connect to Terminal Servers that already have an assigned IP address. To connect to the Terminal Server, type the IP address of the Terminal Server into the **Address** field as such: `http://10.10.234.34`.

You will see the login screen.



The screenshot shows a web-based login interface for a terminal server. At the top left, there is a black header with the 'BLACK BOX' logo. In the top right corner, the text 'TERMINAL SERVER 1 PORT' and 'Version 3.3' is displayed. The main area has a light gray background. In the center, the word 'localhost' is shown above a login form. The form includes a 'Username:' label with a text box containing 'admin', a 'Password:' label with an empty text box, and a 'Login' button below the password field.

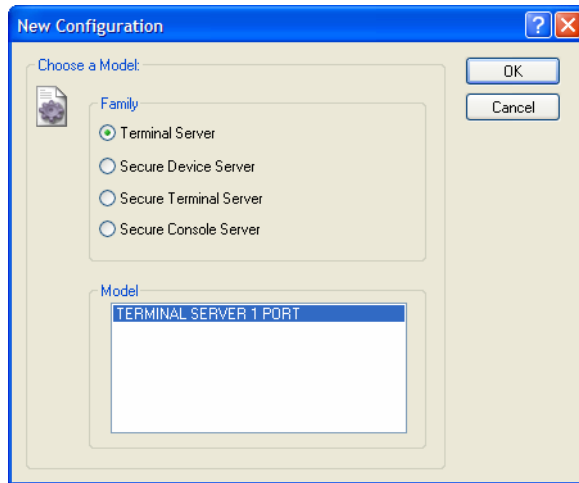
Logging into the Terminal Server

Type in the Admin password in the **Password** field and click the **Login** button.

Configuration Files

Creating a New Terminal Server Configuration in DeviceManager

In DeviceManager, when you select **File, New**, the New Configuration window is displayed.



Select the Terminal Server model for which you want to create a new configuration file. Any configuration file created in this manner can only be save locally. To download a created configuration file, you must first connect to the Terminal Server, import the created configuration file into DeviceManager (this is not available in WebManager), and then download the configuration file to the Terminal Server and reboot it.

Opening an Existing Configuration File

If you select the **File, Open**, a browse window is opened so you can select the configuration file you want to edit. Terminal Server configuration files saved in the DeviceManager can be in the Terminal Server-native binary format (.dme) or as a text file (.txt), which can be edited with a text editor. Either configuration version can be imported into the DeviceManager. Terminal Server configuration files saved from WebManager can also be opened into DeviceManager.

Importing an Existing Configuration File

If you have a local, saved configuration file that you want to download to the Terminal Server, you must first connect to the Terminal Server that you want to download the configuration file to. Once you have successfully logged into the Terminal Server, in DeviceManager select **Tools, Import Configuration from a File** and in WebManager select **Administration, Restore/Backup**. You need to download the file in DeviceManager and in both managers you need to reboot the Terminal Server.

Managing the Terminal Server

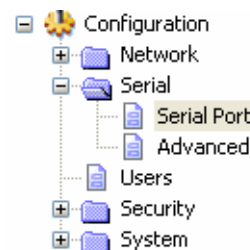
Most of the management tasks, such as setting the time/date, downloading firmware, downloading custom files, resetting serial ports, etc., are found under the **Tools** menu option in the DeviceManager and under **Administration** in WebManager.

6 Configuring Serial Ports

Introduction

The Serial section is used to configure the serial ports on your Terminal Server. The following configuration windows are available:

- **Serial Ports**—This window sets up the type of connection that the serial port is being used for. This is accomplished by selecting a connection profile and then configuring the applicable parameters for that profile. See [Serial Port Profiles](#) for more information.
- **Advanced**—This window configures those parameters that are applicable to specific environments. You will find modem and COMredirect configuration options, in addition to others, here. See [Advanced](#) for more information.



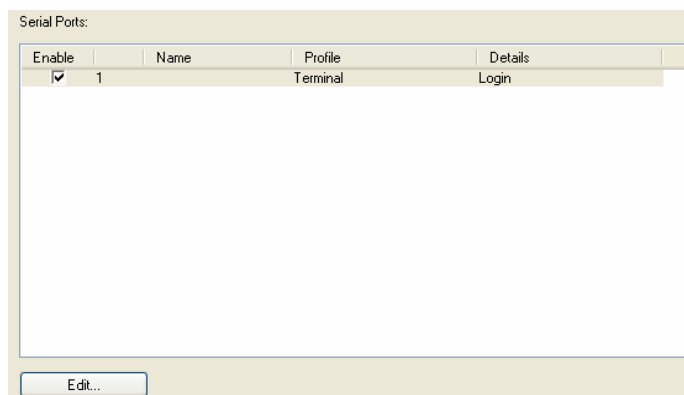
Serial Ports

Overview

Each Terminal Server serial port can be connected to serial device. Each serial port can then be configured according to a serial port profile that coincides with the serial device attached to that serial port and how the serial device is accessed/used.

Functionality

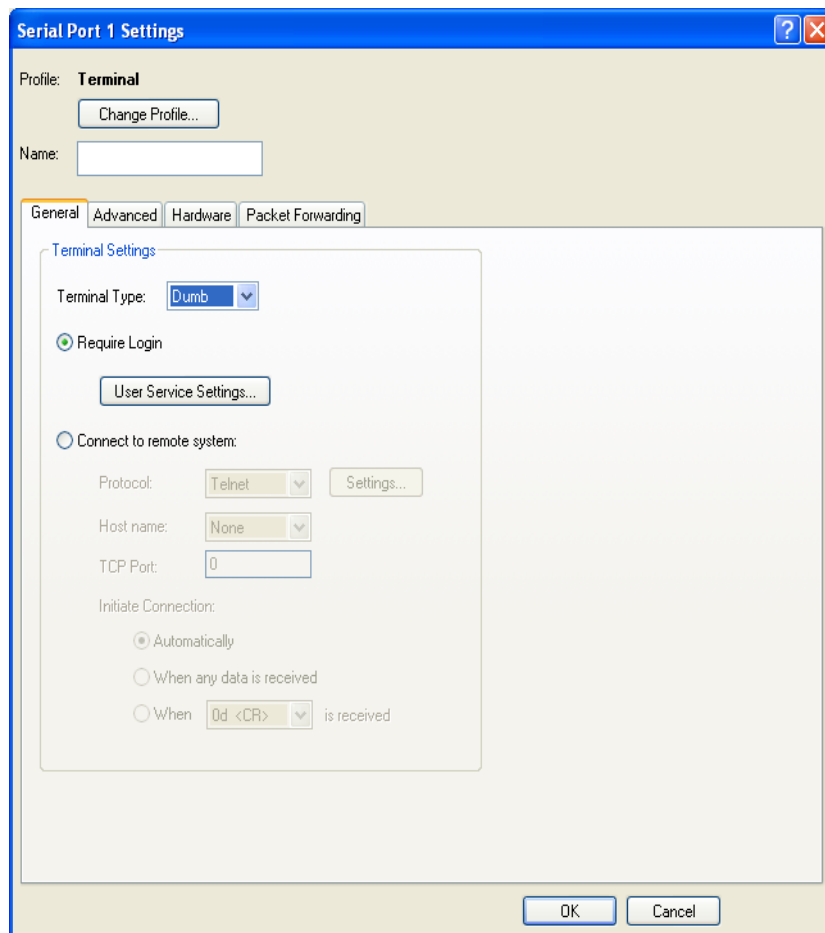
When you select the **Serial Ports** navigation option, you will see a list with the number of serial ports on your Terminal Server. As you configure the serial ports, the information for each serial port is displayed.



To configure/change a serial port, click the **Edit** button.

Editing a Serial Port

In the **Serial Port Settings** window, click on a serial port and then click the **Edit** button, the following window is displayed:



The image shows a Windows-style dialog box titled "Serial Port 1 Settings". It has a blue title bar with a question mark icon and a close button. The main area is divided into four tabs: "General", "Advanced", "Hardware", and "Packet Forwarding". The "General" tab is selected. Inside the "General" tab, there is a "Terminal Settings" section. It includes a "Profile:" label with the value "Terminal" and a "Change Profile..." button. Below that is a "Name:" label followed by an empty text box. The "Terminal Settings" section contains a "Terminal Type:" dropdown menu set to "Dumb". There are two radio buttons: "Require Login" (which is selected) and "Connect to remote system:". Below "Require Login" is a "User Service Settings..." button. Below "Connect to remote system:" are three fields: "Protocol:" (dropdown set to "Telnet" with a "Settings..." button), "Host name:" (dropdown set to "None"), and "TCP Port:" (text box set to "0"). At the bottom of the "Terminal Settings" section is the "Initiate Connection:" section with three radio buttons: "Automatically" (selected), "When any data is received", and "When" followed by a dropdown set to "0d <CR>" and the text "is received". At the bottom of the dialog box are "OK" and "Cancel" buttons.

Serial Port 1 Settings

Profile: **Terminal**
Change Profile...

Name:

General | Advanced | Hardware | Packet Forwarding

Terminal Settings

Terminal Type: **Dumb**

☒ Require Login
User Service Settings...

☐ Connect to remote system:

Protocol: **Telnet** Settings...

Host name: **None**

TCP Port: **0**

Initiate Connection:

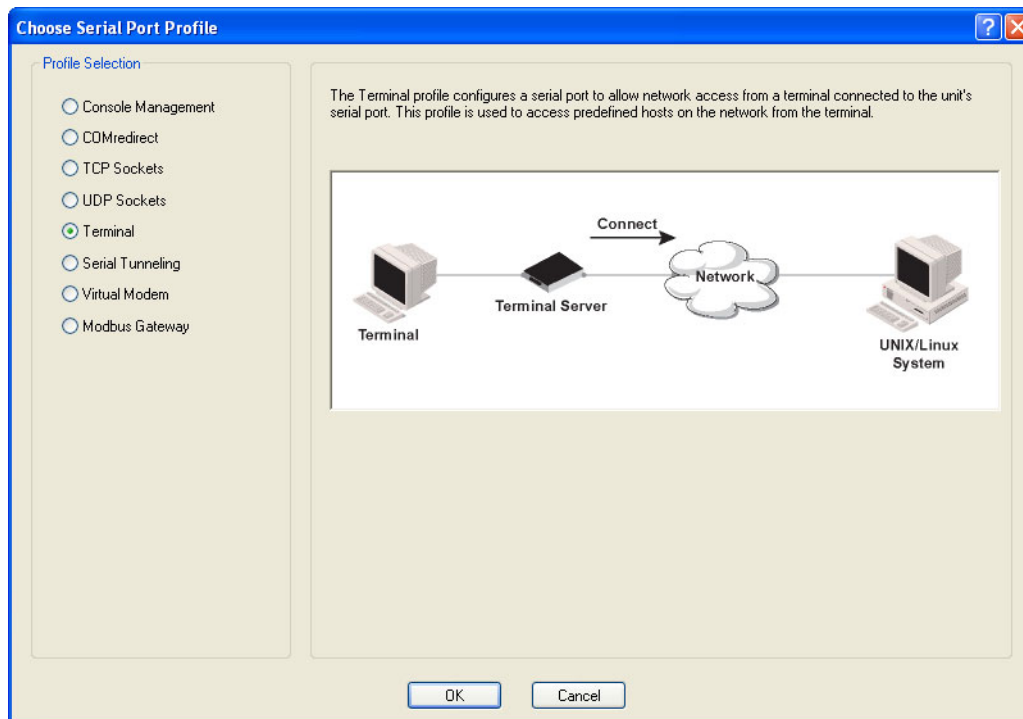
☒ Automatically

☐ When any data is received

☐ When **0d <CR>** is received

OK Cancel

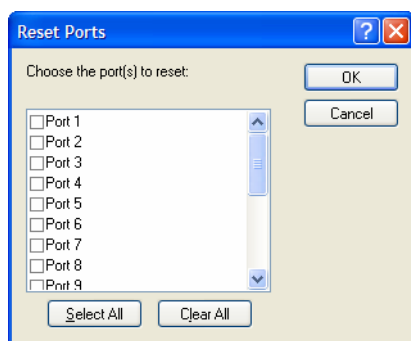
Click the **Change Profile** button to select a different serial port profile if you don't want the displayed profile:



As you select the different serial port profiles, a short description and a picture representing a typical application of the profile is displayed. When you have selected the appropriate profile for the serial port, click **OK** and those serial port profile configuration options will be displayed.

Resetting a Serial Port

When you change a serial port's configuration, you can download the configuration file to the Terminal Server and then reset a specific serial port(s) to see how you change affects the serial port's behavior. To reset a serial port, select **Tools, Reset, Serial Port(s)**.



Serial Port Profiles

Common Tabs

Overview

There are several functions that are common to more than one profile. These functions are:

- **Hardware**—Configure the physical serial line parameters. See [Hardware Tab Field Descriptions](#).
- **Packet Forwarding**—Configure data packet parameters. See [Packet Forwarding Tab Field Descriptions](#).

Hardware Tab Field Descriptions

The **Hardware** tab configures the serial port hardware connection information.

Configure the following parameters:

- | | |
|-------------------------|--|
| Serial Interface | Specifies the type of serial line that is being used with the Terminal Server.
Data Options: EIA-232, EIA-422, or EIA-485. |
| Speed | Specifies the baud rate of the serial line; keep in mind that speed is affected by the length of the cable. You can also specify a custom baud rate. When you enter a custom baud rate, the Terminal Server will calculate the closest baud rate available to the hardware. The exact baud rate calculated can be viewed in the Serial Ports statistics.
Range: 50-230400, custom supports 50-1843200
Default: 9600 |
| Data Bits | Specifies the number of bits in a transmitted character.
Default: 8 |
| Parity | Specifies the type of parity being used for the data communication on the serial port. If you want to force a parity type, you can specify Mark for 1 or Space for 0.
Data Options: Even, Odd, Mark, Space, None
Default: None |

Stop Bits	<p>Specifies the number of stop bits that follow a byte.</p> <p>Data Options: 1, 1.5, 2</p> <p>Default: 1</p>
Duplex	<p>Used with a EIA-485 serial interface, specify whether the serial port is Full Duplex (communication both ways at the same time) or Half Duplex (communication in one direction at a time).</p> <p>Default: Full</p>
TX Driver Control	<p>Used with a EIA-485 serial interface, if your application supports RTS (Request To Send), select this option. Otherwise, select Auto.</p> <p>Default: Auto</p>
Flow Control	<p>Defines whether the data flow is handled by the software (Soft), hardware (Hard), Both, or None.</p> <p>Data Options: Soft, Hard, Both, None</p> <p>Default: None</p>
Enable RTS Toggle	<p>Configure the Toggle RTS feature if your application needs for RTS to be raised during character transmission.</p> <p>Initial Delay: configure the time in (ms) between the time the RTS signal is raised and the start of character transmission. This delay only applies if this port is not running hardware flow control. If hardware flow control is used, the transmission will occur as soon as CTS is raised by the modem.</p> <p>Final Delay: configure the time (in ms) between the time of character transmission and when RTS is dropped.</p> <p>Initial delay range: 1-1000 ms</p> <p>Final delay range: 1-1000 ms</p> <p>Default: off</p>
Enable Inbound Flow Control	<p>Determines if input flow control is to be used.</p> <p>Default: Enabled</p>
Enable Outbound Flow Control	<p>Determines if output flow control is to be used.</p> <p>Default: Enabled</p>
Monitor DSR	<p>Specifies whether the EIA-232 signal DSR (Data Set Ready) should be monitored. This is used with modems or any device that sends a DSR signal. When it is monitored and the Terminal Server detects a DSR signal, the line profile is started. If both Monitor DCD and Monitor DSR are enabled, both signals must be detected before the line profile is started.</p> <p>Default: Disabled</p>
Monitor DCD	<p>Specifies whether the EIA-232 signal DCD (Data Carrier Detect) should be monitored. This is used with modems or any other device that sends a DCD signal. When it is monitored and the Terminal Server detects a DCD signal, the line profile is started. If both Monitor DCD and Monitor DSR are enabled, both signals must be detected before the line profile is started.</p> <p>Default: Disabled</p>

Enable Echo Suppression	<p>This parameter applies only to EIA-485 Half Duplex mode. All characters will be echoed to the user and transmitted across the serial ports. Some EIA-485 applications require local echo to be enabled in order to monitor the loopback data to determine that line contention has occurred. If your application cannot handle loopback data, echo suppression should be enabled.</p> <p>Default: Disabled</p>
Discard Characters with Line Error	<p>When enabled, the Terminal Server will discard characters received with a parity or framing error.</p> <p>Default: Disabled</p>

Packet Forwarding Tab Field Descriptions

The **Packet Forwarding** tab can be used to control/define how and when data packets are sent from the Terminal Server.

Configure the following parameters:

- | | |
|--------------------------------------|---|
| Minimize Latency | This option ensures that any data received on the serial port will immediately be forwarded to the LAN. Select this option for timing-sensitive applications.
Default: Enabled |
| Optimize Network Throughput | This option provides optimal network usage while ensuring that the application performance is not compromised. Select this option when you want to minimize overall packet count, such as when the connection is over a WAN.
Default: Disabled |
| Prevent Message Fragmentation | This option detects the message, packet, or data blocking characteristics of the serial data and preserves it throughout the communication. Select this option for message-based applications or serial devices that are sensitive to inter-character delays within these messages.
Default: Disabled |
| Delay Between Messages | The minimum time, in milliseconds, between messages that must pass before the data is forwarded by the Terminal Server.
Range: 0-65535
Default: 250 ms |
| Custom Packet Forwarding | This option allows you to define the packet forwarding rules based on the packet definition or the frame definition.
Default: Disabled |

Packet Definition	<p>When enabled, this group of parameters allows you to set a variety of packet definition options. The first criteria that is met causes the packet to be transmitted. For example, if you set a Force Transmit Timer of 1000 ms and a Packet Size of 100 bytes, whichever criteria is met first is what will cause the packet to be transmitted.</p> <p>Default: Enabled</p>
Packet Size	<p>The number of bytes that must be received from the serial port before the packet is transmitted to the network. A value of zero (0) ignores this parameter.</p> <p>Range: 0-1024 bytes</p> <p>Default: 0</p>
Idle Time	<p>The amount of time, in milliseconds, that must elapse between characters before the packet is transmitted to the network. A value of zero (0) ignores this parameter.</p> <p>Range: 0-65535 ms</p> <p>Default: 0</p>
Enable Trigger1 Character	<p>When enabled, specifies the character that when received will define when the packet is ready for transmission. The transmission of the packet is based on the Trigger Forwarding Rule.</p> <p>Range: Hex 0-FF</p> <p>Default: 0</p>
Enable Trigger2 Character	<p>When enabled, creates a sequence of characters that must be received to specify when the packet is ready for transmission (if the End Trigger1 character is not immediately followed by the End Trigger2 character, the Terminal Server waits for another End Trigger1 character to start the End Trigger1/End Trigger2 character sequence). The transmission of the packet is based on the Trigger Forwarding Rule.</p> <p>Range: Hex 0-FF</p> <p>Default: 0</p>
Frame Definition	<p>When enabled, this group of parameters allows you to control the frame that is transmitted by defining the start and end of frame character(s). If the internal buffer (1024 bytes) is full before the EOF character(s) are received, the packet will be transmitted and the EOF character(s) search will continue.</p> <p>Default: Disabled</p>
SOF1 Character	<p>When enabled, the Start of Frame character defines the first character of the frame, any character(s) received before the Start of Frame character is ignored.</p> <p>Range: Hex 0-FF</p> <p>Default: 0</p>
SOF2 Character	<p>When enabled, creates a sequence of characters that must be received to create the start of the frame (if the SOF1 character is not immediately followed by the SOF2 character, the Terminal Server waits for another SOF1 character to start the SOF1/SOF2 character sequence).</p> <p>Range: Hex 0-FF</p> <p>Default: 0</p>
Transmit SOF Character(s)	<p>When enabled, the SOF1 or SOF1/SOF2 characters will be transmitted with the frame. If not enabled, the SOF1 or SOF1/SOF2 characters will be stripped from the transmission.</p> <p>Default: Disabled</p>

EOF1 Character	<p>Specifies the End of Frame character, which defines when the frame is ready to be transmitted. The transmission of the frame is based on the Trigger Forwarding Rule.</p> <p>Range: Hex 0-FF</p> <p>Default: 0</p>
EOF2 Character	<p>When enabled, creates a sequence of characters that must be received to define the end of the frame (if the EOF1 character is not immediately followed by the EOF2 character, the Terminal Server waits for another EOF1 character to start the EOF1/EOF2 character sequence), which defines when the frame is ready to be transmitted.</p> <p>Range: Hex 0-FF</p> <p>Default: 0</p>
Trigger Forwarding Rule	<p>Determines what is included in the Frame (based on the EOF1 or EOF1/EOF2) or Packet (based on Trigger1 or Trigger1/Trigger2). Choose one of the following options:</p> <ul style="list-style-type: none"> • Strip-Trigger—Strips out the EOF1, EOF1/EOF2, Trigger1, or Trigger1/Trigger2, depending on your settings. • Trigger—Includes the EOF1, EOF1/EOF2, Trigger1, or Trigger1/Trigger2, depending on your settings. • Trigger+1—Includes the EOF1, EOF1/EOF2, Trigger1, or Trigger1/Trigger2, depending on your settings, plus the first byte that follows the trigger. • Trigger+2—Includes the EOF1, EOF1/EOF2, Trigger1, or Trigger1/Trigger2, depending on your settings, plus the next two bytes received after the trigger. <p>Default: Trigger</p>

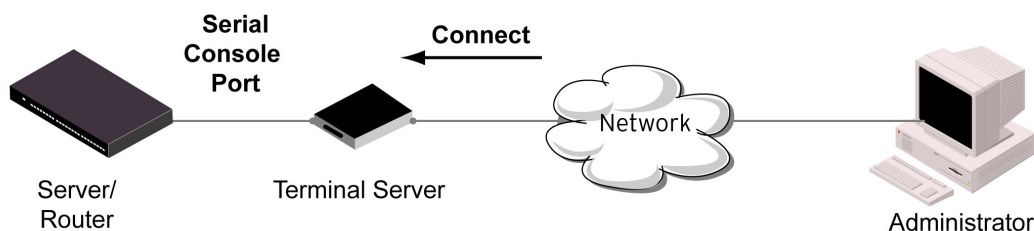
Console Management Profile

Overview

The Console Management profile provides access through the network to a console or administrative port of a server or router attached to the Terminal Server's serial port. This profile configures the Terminal Server's serial port to set up a TCP socket that will listen for a Telnet connection from the network.

Functionality

Use the Console Management profile when you are configuring users who need to access a serial console port from the network.



General Tab Field Descriptions

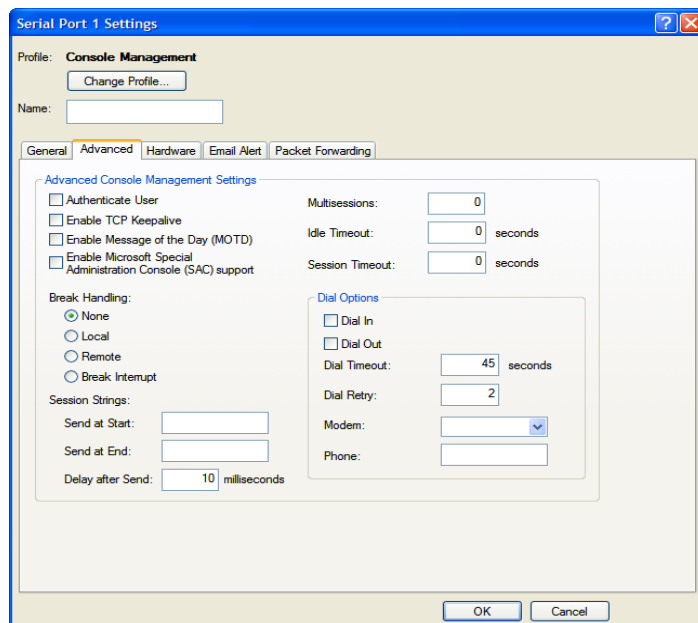
The **Console Management General** tab configures how the serial port will be accessed by the user through the network.

Configure the following parameters:

Protocol	Specify the connection method that users will use to communicate with a serial device connected to the Terminal Server through the network. Default: Telnet
Listen for Connections on TCP Port	The port number that the Terminal Server will listen on for incoming TCP connections. Default: 10001
Enable IP Aliasing	Enables/disables the ability to access a serial device connected to the serial port by an IP address (or host name that can be resolved to an Internet IP Address in a DNS network). The Terminal Server can also be accessed with it's IP address and port number. Default: Disabled
IP Address	Users can access serial devices connected to the Terminal Server through the network by the specified Internet Address (or host name that can be resolved to the Internet Address in a DNS network). Data Options: IPv4 Address

Advanced Tab Field Descriptions

The **Console Management Advanced** tab configures serial port options that may be required by certain applications.



Configure the following parameters:

Authenticate User Enables/disables login/password authentication for users connecting from the network.

Default: Disabled

Enable TCP Keepalive Enables a per-connection TCP keepalive feature. After the configured number of seconds, the connection will send a gratuitous ACK to the network peer, thus either ensuring the connection stays active OR causing a dropped connection condition to be recognized.

This parameter needs to be used in conjunction with **Monitor Connection Status Interval** parameter found in the **Serial, Advanced, Advanced Settings** tab. The interval determines how long the Terminal Server will wait during inactivity before "testing" the connection. It should be noted that if a network connection is accidentally dropped, it can take as long as the specified interval before anyone can reconnect to the serial port.

Default: Disabled

Enable Message of the Day (MOTD) Enables/disables the display of the message of the day.

Default: Disabled

Idle Timeout Use this timer to close a connection because of inactivity. When the **Idle Timeout** expires, the Terminal Server will end the connection.

Default: 0 seconds so the port will never timeout

Range: 0-4294967 seconds (about 49 days)

Session Timeout Use this timer to forcibly close the session/connection when the **Session Timeout** expires.

Default: 0 seconds means the port will never timeout.

Range: 0-4294967 seconds (about 49 days)

Break Handling	<p>Specifies how a break is interpreted.</p> <p>Data Range:</p> <ul style="list-style-type: none"> • None—The Terminal Server ignores the break key completely and it is not passed through to the host. • 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. • Remote—When the break key is pressed, the Terminal Server translates this into a telnet break signal which it sends to the host machine. • Break Interrupt—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 an interrupt key (for example, when the stty options -ignbrk and brkintr are set). <p>Default: None</p>
Session Strings	<p>Controls the sending of ASCII strings to serial devices at session start and session termination as follows;</p> <ul style="list-style-type: none"> • Send at Start—If configured, this string will be sent to the serial device on power-up of the Terminal Server or when a kill line command is issued on this serial port. If the "monitor DSR" or "monitor DCD" options are set the string will also be sent when the monitored signal is raised. Range: 0-127 alpha-numeric characters. Non printable ascii characters must be entered in this format <027>. The decimal numbers within the brackets must be 3 digits long (example 003 not 3). To enter the < (less than symbol) precede the symbol with a \ (backslash symbol). • Send at End—If configured, this string will be sent to the serial device when the TCP session on the LAN is terminated. If multihost is configured, this string will only be sent to the serial device when the profile is configured as a listen mode connection and after all multihost connections are terminated. Non printable ascii characters must be entered in this format <027>. Range: 0-127 alpha-numeric characters. The decimal numbers within the brackets must be 3 digits long (example 003 not 3). To enter the < (less than symbol) precede the symbol with a \ (backslash symbol). • Delay after Send—If configured, a delay time is sent to the device. This delay can be used to provide the serial device with time to process the string before the session is initiated. Range: 0-65535 ms Default: 10 ms
Dial In	<p>If the console port is remote and will be dialing in via modem or ISDN TA, enable this parameter.</p> <p>Default: Disabled</p>
Dial Out	<p>If you want the modem to dial a number when the serial port is started, enable this parameter.</p> <p>Default: Disabled</p>
Dial Timeout	<p>The number of seconds the Terminal Server will wait to establish a connection to a remote modem.</p> <p>Range: 1-99 Default: 45 seconds</p>

Dial Retry	The number of times the Terminal Server will attempt to re-establish a connection with a remote modem. Range: 0-99 Default: 2
Modem	The name of the predefined modem that is used on this line.
Phone	The phone number to use when Dial Out is enabled.

COMredirect Profile

Overview

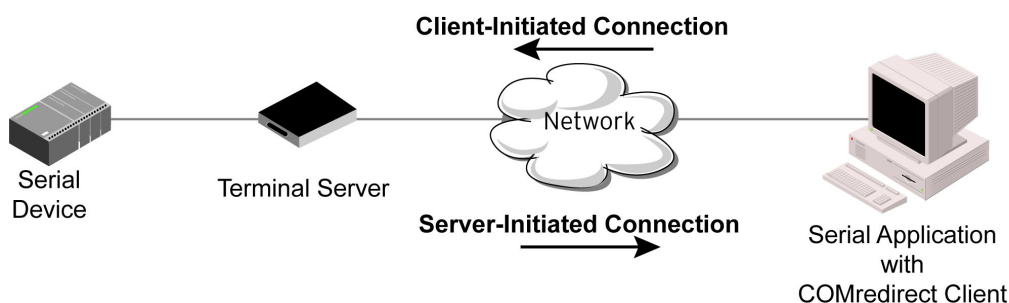
COMredirect is COM Port redirector that is supplied with the Terminal Server. COMredirect can be installed as a client on a Workstation or Server and supports a variety of operating systems. It, in conjunction with the Terminal Server, COMredirect emulates a local serial port (COM port), to the application, to provide connectivity to a remote serial device over the network. The COMredirect profile operates in conjunction with the COMredirect software.

Functionality

COMredirect is a COM port redirector utility for the Terminal Server. It can be run in two modes (these modes will be set on the client software when it is configured):

- **COMredirect Full mode**—This mode allows complete device control and operates as if the device was directly connected to the Workstation/Server's local serial port. It provides a complete COM port interface between the attached serial device and the network. All serial controls, baud rate control, etc., are sent to the Terminal Server and replicated on its associated serial port.
- **COMredirect Lite mode**—This mode provides a simple raw data interface between the application and the remote serial port. Although the port will still operate as a COM port, control signals are ignored. In this mode, the serial communications parameters must be configured on the Terminal Server.

See the *COMredirect User Guide* for more details about the COMredirect client software.



General Tab Field Descriptions

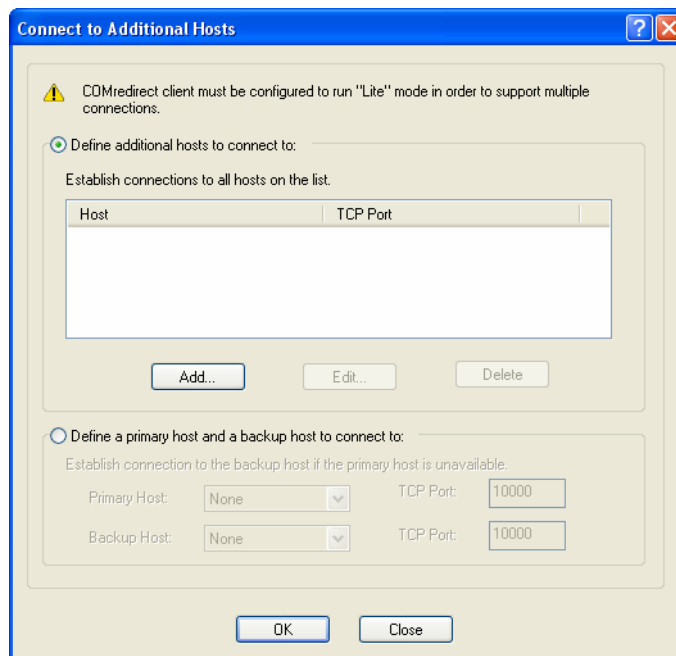
The **COMredirect General** tab determines how the COMredirect connection is initiated and then sets up the appropriate connection parameters.

Configure the following parameters:

Connect to remote system	When enabled, the Terminal Server initiates communication to the COMredirect client. Default: Enabled
Host Name	The configured host that the Terminal Server will connect to (must be running COMredirect). Default: None
TCP Port	The TCP Port that the Terminal Server will use to communicate through to the COMredirect client. Default: 10001 for serial port 1
Connect to Multiple Hosts	When enabled, the Terminal Server will establish a connection to multiple clients (Hosts). When using the multiple hosts feature, all COMredirect clients must be running in Lite mode. Default: Disabled
Send Name on Connect	When enabled, the port name will be sent to the host upon session initiation. Default: Disabled.
Define Additional Hosts Button	Click this button to define the hosts that this serial port will connect to. This button is also used to define the Primary/Backup host functionality. See Adding/Editing Additional COMredirect Hosts for more information.
Listen for Connection	When enabled, the Terminal Server will wait for connections to be initiated by the COMredirect Client. Default: Disabled
TCP Port	The TCP Port that the Terminal Server will use to communicate through to the COMredirect client. Default: 10001 for serial port 1
Allow Multiple Hosts to Connect	When this option is enabled, multiple hosts can connect to a serial device that is connected to this serial port. Note: These multiple clients (Hosts) need to be running COMredirect in Lite mode. Default: Disabled

Adding/Editing Additional COMredirect Hosts

You can define a list of hosts that the serial device will communicate to through COMredirect Lite or a primary/backup host.



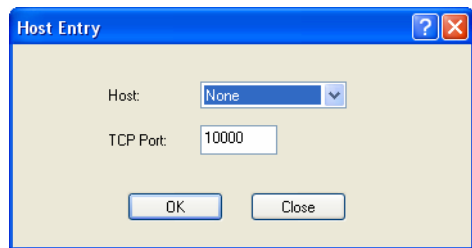
Configure the following parameters:

- | | |
|--|--|
| Define additional hosts to connect to | When this option is enabled, you can define up to 49 hosts that the serial device connected to this serial port will attempt communicate to. With this mode of operation, the Terminal Server will connect to multiple hosts simultaneously.
Default: Enabled |
| Add Button | Click the Add button to add a host to the list of hosts that will be receiving communication from the serial device connected to the Terminal Server.
See Adding/Editing a Multihost Entry for more information. |
| Edit Button | Highlight an existing host and click the Edit button to edit a host in the list of hosts that will be receiving communication from the serial device connected to the Terminal Server. |
| Delete Button | Highlight an existing host and click the Edit button to edit a host in the list of hosts that will be receiving communication from the serial device connected to the Terminal Server. |
| Define a primary host and backup... | When this option is enabled, you need to define a primary host that the serial device connected to this serial port will communicate to and a backup host, in the event that the Terminal Server loses communication to the primary host. The Terminal Server will first establish a connection to the primary host. Should the connection to the primary host be lost (or never established), the Terminal Server will establish a connection the backup host. Once connected to the backup, the Terminal Server will attempt to re-establish a connection to the Primary host, once this is successfully done, it gracefully shuts down the backup connection.
Default: Disabled |

Primary Host	Specify a preconfigured host that the serial device will communicate to through the Terminal Server. Default: None
TCP Port	Specify the TCP port that the Terminal Server will use to communicate to the Primary Host . Default: 0
Backup Host	Specify a preconfigured host that the serial device will communicate to through the Terminal Server if the Terminal Server cannot communicate with the Primary Host . Default: None
TCP Port	Specify the TCP port that the Terminal Server will use to communicate to the Backup Host . Default: 10000

Adding/Editing a Multihost Entry

When you click the **Add** or **Edit** button, the Host Entry window appears. The hosts in the multihost list must already be defined. If you add a host that was defined with its fully qualified domain name (FQDN), it must be resolvable by your configured DNS server.



Configure the following parameters:

Host Name	Specify the preconfigured host that will be in the multihost list. Default: None
TCP Port	Specify the TCP port that the Terminal Server will use to communicate to the Primary Host . Default: 10000 + serial port number - 1 (so serial port 2 defaults to 10001)

Advanced Tab Field Descriptions

The **COMredirect Advanced** tab determines how the COMredirect connection is initiated and then sets up the appropriate connection parameters.

Configure the following parameters:

Signals high when...

This option has the following impact based on the state of the COMredirect connection:

- **COMredirect Lite Mode**—When enabled, the EIA-232 signals remain active before, during, and after the COMredirect connection is established. When disabled, the EIA-232 signals remain inactive during and after the COMredirect connection is established.
- **COMredirect Full Mode**—When enabled, the EIA-232 signals remain active before and after the COMredirect connection and the COMredirect client will control the state of the signals during the established COMredirect connection. When disabled, the EIA-232 signals remain inactive before and after the COMredirect connection and the COMredirect client will control the state of the signals during the established COMredirect connection.

Default: Enabled

Enable Message of the Day (MOTD)

Enables/disables the display of the message of the day.

Default: Disabled

Enable TCP Keepalive

Enables a per-connection TCP keepalive feature. After the configured number of seconds, the connection will send a gratuitous ACK to the network peer, thus either ensuring the connection stays active OR causing a dropped connection condition to be recognized.

This parameter needs to be used in conjunction with **Monitor Connection Status Interval** parameter found in the **Serial, Advanced, Advanced Settings** tab. The interval determines how long the Terminal Server will wait during inactivity before "testing" the connection. It should be noted that if a network connection is accidentally dropped, it can take as long as the specified interval before anyone can reconnect to the serial port.

Default: Disabled

Enable Data Logging [COMredirect Lite Mode]	<p>When enabled, serial data will be buffered if the TCP connection is lost. When the TCP connection is re-established, the buffered serial data will be sent to its destination. Only valid in COMredirect LITE Mode. Not valid when using COMredirect in Full mode.</p> <p>The minimum data buffer size is 1 KB for all models. The maximum data buffer size is 2000 KB for the TS1, all other models are 4000 KB. If the data buffer is filled, incoming serial data will overwrite the oldest data.</p> <p>Values: 1-2000 KB (TS1) default 4 KB</p> <p>Values: 1-4000 KB (all other models) default 256</p> <p>Some profile feature are not compatible with Data Logging. See Appendix G, Data Logging for the complete list.</p> <p>Note: A kill line or reboot of the Terminal Server causes all buffered data to be lost.</p> <p>To change the default buffer size see Advanced Serial Settings Tab</p> <p>Default: Disabled</p>
Idle Timeout	<p>Use this timer to close a connection because of inactivity. When the Idle Timeout expires, the Terminal Server will end the connection.</p> <p>Default: 0 seconds so the port will never timeout</p> <p>Range: 0-4294967 seconds (about 49 days)</p>
Session Timeout	<p>Use this timer to forcibly close the session/connection when the Session Timeout expires.</p> <p>Default: 0 seconds so the port will never timeout</p> <p>Range: 0-4294967 seconds (about 49 days)</p>
Session Strings	<p>Controls the sending of ASCII strings to serial devices at session start as follows;</p> <ul style="list-style-type: none"> <p>Send at Start—If configured, this string will be sent to the serial device on power-up of the Terminal Server or when a kill line command is issued on this serial port. If the "monitor DSR" or "monitor DCD" options are set, the string will also be sent when the monitored signal is raised.</p> <p>Range: 0-127 alpha-numeric characters</p> <p>Range: hexadecimal 0-FF</p> <p>Delay after Send—If configured, will inset a delay after the string is sent to the device. This delay can be used to provide the serial device with time to process the string before the session is initiated or terminated.</p> <p>Default: 10 ms</p>
Dial In	<p>If the device is remote and will be dialing in via modem or ISDN TA, enable this parameter.</p> <p>Default: Disabled</p>
Dial Out	<p>If you want the modem to dial a number when the serial port is started, enable this parameter.</p> <p>Default: Disabled</p>
Dial Timeout	<p>The number of seconds the Terminal Server will wait to establish a connection to a remote modem.</p> <p>Range: 1-99</p> <p>Default: 45 seconds</p>

Dial Retry	The number of times the Terminal Server will attempt to re-establish a connection with a remote modem. Range: 0-99 Default: 2
Modem	The name of the predefined modem that is used on this line.
Phone	The phone number to use when Dial Out is enabled.

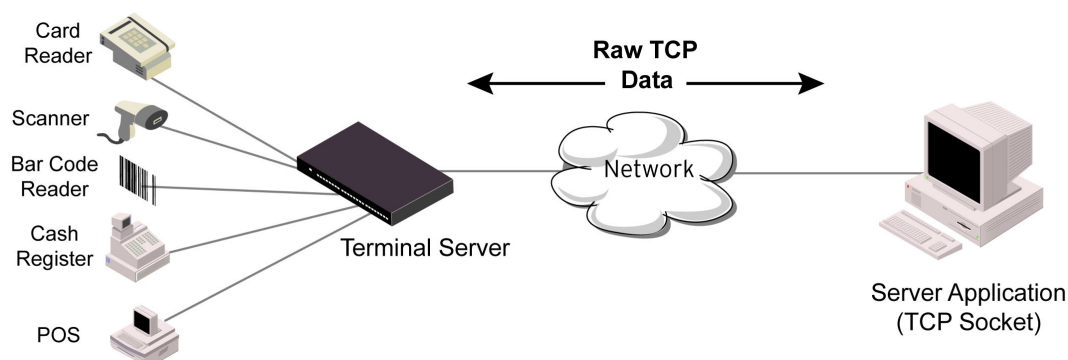
TCP Sockets Profile

Overview

The TCP Socket profile allows for a serial device to communicate over a TCP network. The TCP connection can be initiated from a host on the network and/or a serial device. This is typically used with an application on a Workstation or Server that communicates to a device using a specific TCP socket. This is often referred to as a RAW connection.

Functionality

The **TCP Sockets** profile permits a raw connection to be established in either direction, meaning that the connection can be initiated by either the Workstation/Server or the Terminal Server.



General Tab Field Descriptions

Serial Port 1 Settings

Profile: **TCP Sockets**

Name:

General | Advanced | Hardware | Email Alert | Packet Forwarding | SSL/TLS

TCP Socket Settings

☒ Listen for connection:
 TCP Port:
☐ Allow Multiple Hosts to Connect
☐ Enable IP Aliasing
 IP Address:

☐ Connect to:
 Host name: TCP Port:
☐ Connect to Multiple Hosts

Initiate Connection:
☒ Automatically
☐ When any data is received
☐ When is received
☐ Send Name On Connect

☐ Permit Connections in Both Directions

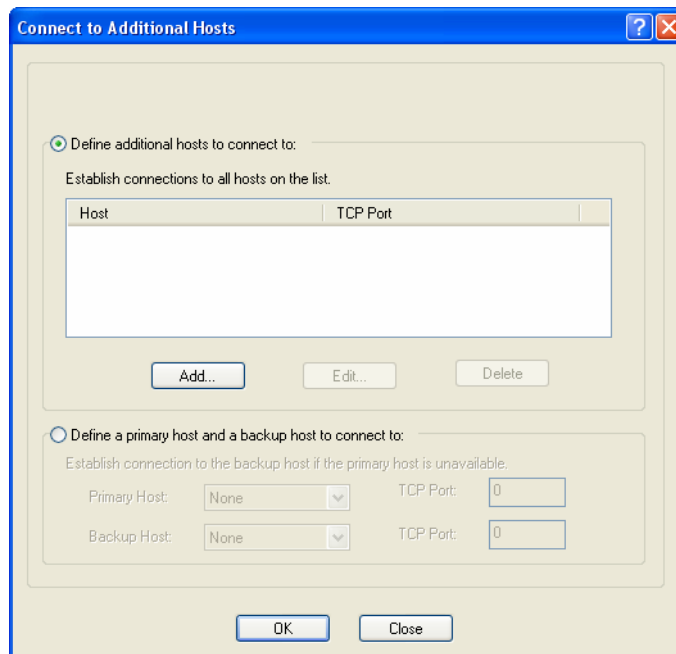
Configure the following parameters:

Listen for Connection	When enabled, the Terminal Server listens for a connection to be established by the Workstation/Server on the network. Default: Enabled
TCP Port	The TCP port that the Terminal Server will use to listen for incoming connections. Default: 10000 plus the serial port number, so serial port 2 would have a default of 10002
Allow Multiple Hosts to Connect	When this option is enabled, multiple hosts can connect to the serial device that is connected to this serial port. Default: Disabled
Enable IP Aliasing	Enables/disables the ability to access a serial device connected to the serial port by an IP address (or host name that can be resolved to an Internet IP Address in a DNS network). The Terminal Server can also be accessed with it's IP address and port number. Default: Disabled
Connect To	When enabled, the Terminal Server initiates communication to the Workstation/Server. Default: Disabled
Host Name	The name (resolvable via DNS) or IP address of the configured host the Terminal Server will connect to.

TCP Port	The TCP Port that the Terminal Server will use to communicate to the client. Default: 0
Connect to Multiple Hosts	When enabled, allows a serial device connected to this serial port to communicate to multiple hosts. Default: Disabled
Define Additional Hosts Button	Click this button to define the hosts that this serial port will connect to. This button is also used to define the Primary/Backup host functionality.
Initiate Connection Automatically	If the serial port hardware parameters have been setup to monitor DSR or DCD, the host session will be started once the signals are detected. If no hardware signals are being monitored, the Terminal Server will initiate the session immediately after being powered up. Default: Enabled
Initiate Connection When any data is received	Initiates a connection to the specified host when any data is received on the serial port. Default: Disabled
Initiate Connection When <hex value> is received	Initiates a connection to the specified host only when the specified character is received on the serial port. Default: Disabled
Permit Connections in Both Directions	When this option is enabled, you can select both checkbox options "listen for connection" and "connect to". Default: Disabled

Adding/Editing Additional Hosts

You can define a list of hosts that the serial device will communicate to or a primary/backup host.



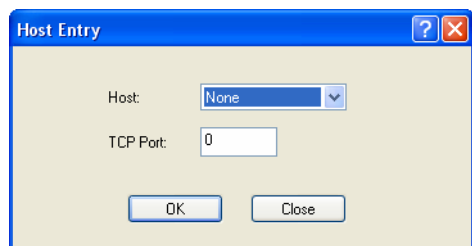
Configure the following parameters:

- | | |
|--|--|
| Define additional hosts to connect to | When this option is enabled, you can define up to 49 hosts that the serial device connected to this serial port will attempt communicate to. With this mode of operation, the Terminal Server will connect to multiple hosts simultaneously.
Default: Enabled |
| Add Button | Click the Add button to add a host to the list of hosts that will be receiving communication from the serial device connected to the Terminal Server. |
| Edit Button | Highlight an existing host and click the Edit button to edit a host in the list of hosts that will be receiving communication from the serial device connected to the Terminal Server. |
| Delete Button | Click the Delete button to delete a host to the list of hosts that will be receiving communication from the serial device connected to the Terminal Server. |
| Define a primary host and backup... | When this option is enabled, you need to define a primary host that the serial device connected to this serial port will communicate to and a backup host, in the event that the Terminal Server loses communication to the primary host. The Terminal Server will first establish a connection to the primary host. Should the connection to the primary host be lost (or never established), the Terminal Server will establish a connection the backup host. Once connected to the backup, the Terminal Server will attempt to re-establish a connection to the Primary host, once this is successfully done, it gracefully shuts down the backup connection.
Default: Disabled |
| Primary Host | Specify a preconfigured host that the serial device will communicate to through the Terminal Server.
Default: None |

TCP Port	Specify the TCP port that the Terminal Server will use to communicate to the Primary Host . Default: 0
Backup Host	Specify a preconfigured host that the serial device will communicate to through the Terminal Server if the Terminal Server cannot communicate with the Primary Host . Default: None
TCP Port	Specify the TCP port that the Terminal Server will use to communicate to the Backup Host . Default: 10000

Adding/Editing a Multihost Entry

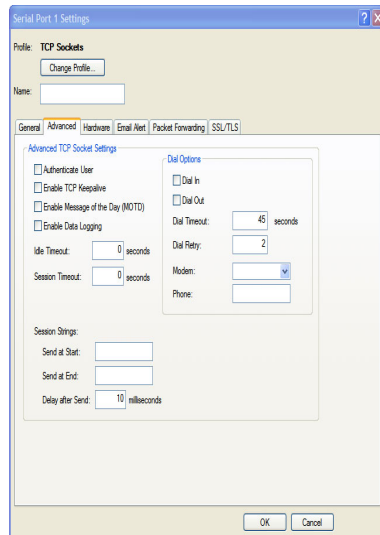
When you click the **Add** or **Edit** button, the Host Entry window appears. The hosts in the multihost list must already be defined (see [Host Table](#) to learn how to create a host). If you add a host that was defined with its fully qualified domain name (FQDN), it must be resolvable by your configured DNS server.



Configure the following parameters:

Host Name	Specify the preconfigured host that will be in the multihost list. Default: None
TCP Port	Specify the TCP port that the Terminal Server will use to communicate to the Host . Default: 0

Advanced Tab Field Descriptions



Configure the following parameters:

- | | |
|---|--|
| Authenticate User | Enables/disables login/password authentication for users connecting from the network.
Default: Disabled |
| Enable TCP Keepalive | Enables a per-connection TCP keepalive feature. After the configured number of seconds, the connection will send a gratuitous ACK to the network peer, thus either ensuring the connection stays active OR causing a dropped connection condition to be recognized.

This parameter needs to be used in conjunction with Monitor Connection Status Interval parameter found in the Serial, Advanced, Advanced Settings tab. The interval determines how long the Terminal Server will wait during inactivity before "testing" the connection. It should be noted that if a network connection is accidentally dropped, it can take as long as the specified interval before anyone can reconnect to the serial port.
Default: Disabled |
| Enable Message of the Day (MOTD) | Enables/disables the display of the message of the day.
Default: Disabled |
| Idle Timeout | Use this timer to close a connection because of inactivity. When the Idle Timeout expires, the Terminal Server will end the connection.
Default: 0 seconds so the port will never timeout
Range: 0-4294967 seconds (about 49 days) |
| Session Timeout | Use this timer to forcibly close the session/connection when the Session Timeout expires.
Default: 0 seconds so the port will never timeout
Range: 0-4294967 seconds (about 49 days) |

Enable Data Logging	<p>When enabled, serial data will be buffered if the TCP connection is lost. When the TCP connection is re-established, the buffered serial data will be sent to its destination.</p> <p>The minimum data buffer size is 1 K for all desktop models and the maximum data buffer size is 2 MB. If the data buffer is filled, incoming serial data will overwrite the oldest data.</p> <p>The minimum data buffer size is 1 KB for all models. The maximum data buffer size is 2000 KB for the TS1, all other models are 4000 KB. If the data buffer is filled, incoming serial data will overwrite the oldest data.</p> <p>Values: 1-2000 KB (TS1) default 4 KB</p> <p>Values: 1-4000 KB (all other models) default 256 KB</p> <p>Some profile feature are not compatible with Data Logging. See Appendix G, Data Logging for the complete list.</p> <p>Note: A kill line or reboot of the Terminal Server causes all buffered data to be lost.</p> <p>To change the default buffer size see Advanced Serial Settings Tab</p>
Sessions Strings	<p>Default: Disabled</p> <p>Controls the sending of ASCII strings to serial devices at session start and session termination as follows;</p> <ul style="list-style-type: none"> <p>Send at Start—If configured, this string will be sent to the serial device on power-up of the Terminal Server or when a kill line command is issued on this serial port. If the "monitor DSR" or "monitor DCD" options are set the string will also be sent when the monitored signal is raised.</p> <p>Range: 0-127 alpha-numeric characters. Non printable ascii characters must be entered in this format <027>. The decimal numbers within the brackets must be 3 digits long (example 003 not 3). To enter the < (less than symbol) precede the symbol with a \ (backslash symbol).</p> <p>Send at End—If configured, this string will be sent to the serial device when the TCP session on the LAN is terminated. If multihost is configured, this string will only be sent to the serial device when the profile is configured as a listen mode connection and after all multihost connections are terminated. Non printable ascii characters must be entered in this format <027>.</p> <p>Range: 0-127 alpha-numeric characters. The decimal numbers within the brackets must be 3 digits long (example 003 not 3). To enter the < (less than symbol) precede the symbol with a \ (backslash symbol).</p> <p>Delay after Send—If configured, a delay time is sent to the device. This delay can be used to provide the serial device with time to process the string before the session is initiated.</p> <p>Range: 0-65535 ms</p> <p>Default: 10 ms</p>
Dial In	<p>If the device is remote and will be dialing in via modem or ISDN TA, enable this parameter.</p> <p>Default: Disabled</p>
Dial Out	<p>If you want the modem to dial a number when the serial port is started, enable this parameter.</p> <p>Default: Disabled</p>

Dial Timeout	The number of seconds the Terminal Server will wait to establish a connection to a remote modem. Range: 1-99 Default: 45 seconds
Dial Retry	The number of times the Terminal Server will attempt to re-establish a connection with a remote modem. Range: 0-99 Default: 2
Modem	The name of the predefined modem that is used on this line.
Phone	The phone number to use when Dial Out is enabled.

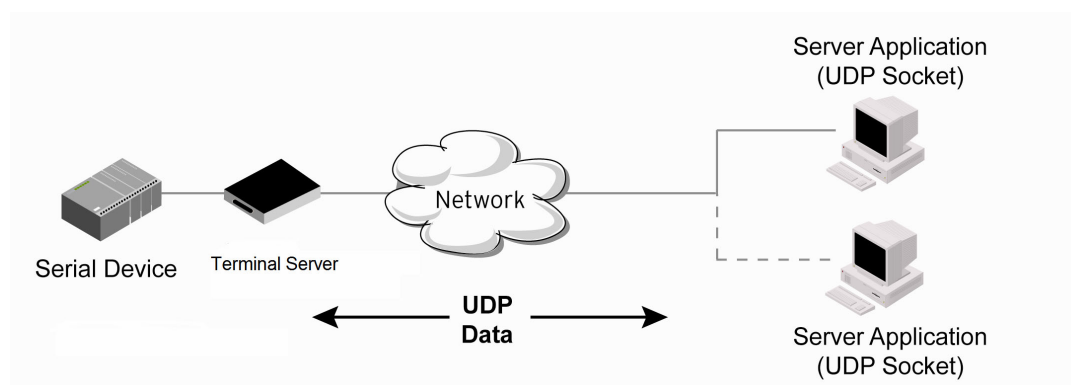
UDP Sockets Profile

Overview

When you configure **UDP**, you are setting up a range of IP addresses and the port numbers that you will use to send UDP data to or receive UDP data from.

Functionality

You can use UDP profile in the following two basic modes. The first is to send data coming from the serial device to one or more UDP listeners on the LAN. The second is to accept UDP datagrams coming from one or more UDP senders on the LAN and forward this data to the serial device. You can also configure a combination of both which will allow you to send and receive UDP data to/from the LAN.



Sample **UDP Sockets** configuration screen

General Hardware Email Alert Packet Forwarding

UDP Socket Settings

Listen for connections on UDP port:

Host Range

	Direction	Start IP Address	End IP Address	UDP Port
1	Both	0.0.0.0	0.0.0.0	Auto Learn
2	Disabled	0.0.0.0	0.0.0.0	Auto Learn
3	Disabled	0.0.0.0	0.0.0.0	Auto Learn
4	Disabled	0.0.0.0	0.0.0.0	Auto Learn

Four individual entries are provided to allow you greater flexibility to specify how data will be forwarded to/from the serial device. All four entries support the same configuration parameters. You can configure one or more of the entries as needed.

The first thing you need to configure for an entry is the “**Direction**” of the data flow. The following options are available;

- **Disabled** - UDP service not enabled.
- **LAN to Serial** - This setting will allow UDP data to be received from one or more hosts on the LAN and forwarded to the serial device attached to this serial port.
- **Serial to LAN** - This setting will allow data originating from the serial device attached to this serial port to be sent to one or more hosts on the LAN using UDP datagrams.
- **Both** - Allows for data to flow from the serial device to the LAN and from the LAN to the serial device.

The role of each of the configurable parameters in an entry depends on the “**Direction**” selected.

When the direction is “**LAN to Serial**” the role of the additional parameters is as follow;

- **Start IP Address** - This is the IP address of the host from which the UDP data will originate. If the data will originate from a number of hosts, this becomes the starting IP address of a range.
- **End IP Address** - If you wish to receive data only from the single host defined by “Start IP address”, leave this entry as is (0.0.0.0). If you wish to accept data from a number of hosts, this address will represent the upper end of a range starting from “Start IP Address”. Only data originating from this range will be forwarded to the serial port.
- **UDP port** - This is the UDP port from which the data will originate. There are three options for this parameter.
 - **Auto Learn** - The first UDP message received will be used to define which UDP port we are going to accept UDP data from. Once learned, only data from this UDP port will be accepted. The data must also originate from a host which is in the IP range defined for this entry.
 - **Any Port** - Any UDP port will be accepted as long as the data originates from a host in the IP range defined for this entry.
 - **Port** - Only data originating from the UDP port configured here as well as originating from a host in the IP range defined for this entry will be accepted.

When the direction is “**Serial to LAN**” the role of the additional parameters is as follow;

- **Start IP Address** - This is the IP address of the host to which the serial data will be sent using UDP datagrams. If the serial data is to be sent to more than one host, this becomes the starting IP address of a range.
- **End IP Address** - If you wish to send serial data to a single host, leave this entry as is (0.0.0.0). If you wish to send the serial data to a number of hosts, this address will represent the upper end of a range starting from “Start IP Address”.
- **UDP port** - This is the UDP port to which the serial data will be forwarded. For a direction of “Serial to LAN”, you must specify the port to be used.

When the direction is “**Both**” the role of the additional parameters is as follow;

- **Start IP Address** - This is the IP address of the host to which the serial data will be sent using UDP datagrams. It is also the IP address of the host from which UDP data coming from the LAN will be accepted from. If the data is to be sent to or received from more than one host, this becomes the starting IP address of a range.
- **End IP Address** - If you wish to send serial data to a single host and only receive data from the single UDP host, leave this entry as is (0.0.0.0). If the data is to be sent to or received from more than one host, this address will represent the upper end of a range starting from “Start IP Address”. Only data originating from this range will be forwarded to the serial port.

- **UDP Port** - This is the UDP port to which the serial data will be forwarded as well as the UDP port from which data originating on the LAN will be accepted from. For a direction of "Both", there are two valid option for the UDP Port as follows;
 - **Auto Learn** - The first UDP message received will be used to define which port we are going to accept UDP data from. Once learned, only data from this UDP port will be accepted and serial data being forwarded to the LAN will be sent to this UDP port. Until the port is learned, data from the serial port intended to be sent to the LAN will be discarded.
 - **Port** - Serial data being forwarded to the LAN from the serial device will sent to this UDP port. Only data originating from the UDP port configured here (as well as originating from a host in the IP range defined for this entry) will be forwarded to the serial device.

Special values for "Start IP address"

- **0.0.0.0** - This is the "auto learn IP address" value which is valid only in conjunction with the "LAN to Serial" setting. The first UDP packet received for this serial port will set the IP address from which we will accept future UDP packets to be forwarded to the serial port. For this setting, leave the "End IP Address" as 0.0.0.0.
- **255.255.255.255** - This selection is only valid in conjunction with the "LAN to Serial" setting. It will accept all UDP packets received for this serial port regardless of the originating IP address. For this setting, leave the "End IP Address" as 0.0.0.0.
- **Subnet directed broadcast** - You can use the "Start IP Address" field to enter a subnet directed broadcast address. This is done by specifying the subnet address with the host portion filled with 1s. For example, if you are on the subnet 172.16.x.x with a subnet mask of 255.255.254.0 than you would specify an IP address of 172.16.1.255 (all ones for host portion). For this setting, leave the "End IP Address" as 0.0.0.0. For any "LAN to Serial" ranges you have defined for this serial port, you must ensure that IP address of this Terminal Server is not included in the range. If your IP address is within the range, you will receive the data you send via the subnet directed broadcasts as data coming in from the LAN.

An example UDP configuration is described based on the following window.

Direction	Start IP Address	End IP Address	UDP Port
1 LAN to Serial	172.16.1.25	172.16.1.50	33010
2 Serial to LAN	172.16.1.75	172.16.1.80	33009
3 Both	172.16.1.1	172.16.1.20	33001
4 Disabled	0.0.0.0	0.0.0.0	0

The UDP configuration window, taken from the DeviceManager, is configured to:

- **UDP Entry 1**
All UDP data received from hosts that have an IP address that falls within the range of **172.16.1.25 to 172.16.1.50** and source UDP **Port 33010** will be sent to the serial device. The Terminal Server will not send any data received on its serial port to the host range defined by this entry.
- **UDP Entry 2**
All hosts that have an IP Address that falls within the range of **172.16.1.75 to 172.16.1.80** and who listen to UDP **Port 33009** will receive UDP data from the serial device. No UDP data originating from the hosts defined by this entry will be forwarded to the serial device.
- **UDP Entry 3**

All hosts that have an IP address that falls within the range of **172.16.1.1** to **172.16.1.20** and listen to **Port 33001** will be sent the data from the serial device in UDP format. The serial device will only receive UDP data from the hosts in that range with a source UDP **Port** of **33001**. The Terminal Server will listen for data on the port value configured in the **Listen for connections on UDP port** parameter. (10001 in above example)

- **UDP Entry 4**

This entry is disabled since **Direction** is set to **Disabled**.

General Tab Field Descriptions

UDP Socket Settings				
Listen for connections on UDP port: 10001				
Host Range				
	Direction	Start IP Address	End IP Address	UDP Port
1	Both		0.0.0.0	Auto Learn 0
2	Disabled		0.0.0.0	Auto Learn 0
3	Disabled		0.0.0.0	Auto Learn 0
4	Disabled		0.0.0.0	Auto Learn 0

Configure the following parameters:

Listen for connections on UDP port

The Terminal Server will listen for UDP packets on the specified port.

Default: 1000

Direction

The direction in which information is received or relayed:

- **Disabled**—UDP service not enabled.
- **LAN to Serial—UDP Port** can be set to **Auto Learn** or **Port**. The Terminal Server will listen on port value configured in the **Listen for connections on UDP port** parameter for messages coming from the learned or configured port.
- **Serial to LAN—UDP Port** can be set to **Port** only. The Terminal Server will listen on the port value configured in the **Listen for connections on UDP port** parameter and will send to the configured port.
- **Both**—Messages are relayed in both directions. UDP Port can be set to **Auto Learn** or **Port**. For messages coming from the LAN to the serial device, Terminal Server will listen on port value configured in the **Listen for connections on UDP port** parameter for messages coming from the learned or configured port. For messages going from the serial device to the LAN, the Terminal Server will listen on the port value configured in the **Listen for connections on UDP port** parameter and will send to the configured or learned (if **Auto Learn** is enabled, the Terminal Server must receive a UDP message before it can send one, since the port must first be ('learned') port.
- **Default:** Both for UDP 1 and Disabled for all other UDP ranges

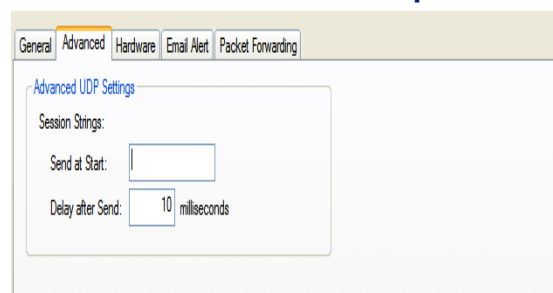
Start IP Address

The first host IP address in the range of IP addresses (for IPV4 or IPV6) that the Terminal Server will listen for messages from and/or send messages to.

Field Format: IPv4 or IPv6 address

End IP Address	<p>The last host IP address in the range of IP addresses (for IPV4, not required for IPV6) that the Terminal Server will listen for messages from and/or send messages to.</p> <p>Field Format: IPv4 address</p>
UDP Port	<p>Determines how the Terminal Server's UDP port that will send/receive UDP messages is defined:</p> <ul style="list-style-type: none"> • Auto Learn—The Terminal Server will only listen to the first port that it receives a UDP packet from. Applicable when Direction is set to LAN to Serial or Both. • Any Port—The Terminal Server will receive messages from any port sending UDP packets. Applicable when Direction is set to LAN to Serial. • Port—The port that the Terminal Server will use to relay messages to servers/hosts. This option works with any Direction except Disabled. The Terminal Server will listen for UDP packets on the port configured by the Listen for connections on UDP port parameter. <p>Default: Auto Learn</p>
Port	<p>The port that the Terminal Server will use to relay messages to servers/hosts. This option works with any Direction except Disabled. The Terminal Server will listen for UDP packets on the port configured by the Listen for connections on UDP port parameter.</p> <p>Default: 0 (zero)</p>

Advanced Tab Field Descriptions



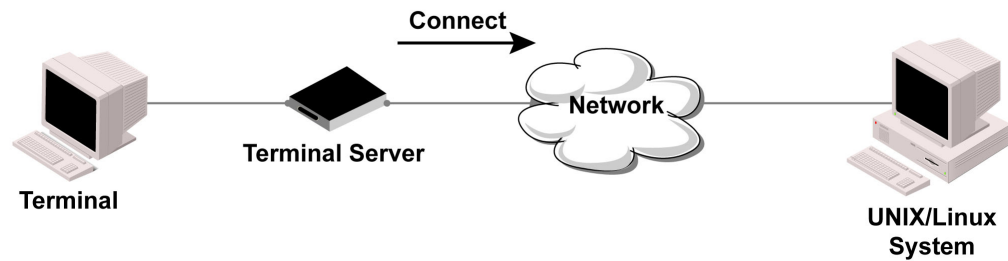
Configure the following parameters:

Session Strings	<p>Controls the sending of ASCII strings to serial devices at session start as follows;</p> <ul style="list-style-type: none"> • Send at Start—If configured, this string will be sent to the serial device on power-up of the Terminal Server or when a kill line command is issued on this serial port. If the "monitor DSR" or "monitor DCD" options are set, the string will also be sent when the monitored signal is raised. Range: 0-127 alpha-numeric characters Range: hexadecimal 0-FF • Delay after Send—If configured, will inset a delay after the string is sent to the device. This delay can be used to provide the serial device with time to process the string before the session is initiated or terminated. Default: 10 ms
------------------------	--

Terminal Profile

Overview

The Terminal profile allows network access from a terminal connected to the Terminal Server's serial port. This profile is used to access pre-defined hosts on the network from the terminal.



Functionality

This profile can be setup in two ways:

1. The user can be required to log into the Terminal Server and then a connection to a host can be established.
2. The user connecting to the serial port will be directly connected a host.

General Tab Field Descriptions

General Advanced Hardware Packet Forwarding

Terminal Settings

Terminal Type: Dumb

☒ Require Login

User Service Settings...

☐ Connect to remote system:

Protocol: Telnet Settings...

Host name: None

TCP Port: 0

Initiate Connection:

☒ Automatically

☐ When any data is received

☐ When 0d <CR> is received

Configure the following parameters:

Terminal Type	<p>Specifies the type of terminal connected to the line.</p> <p>Data Options:</p> <ul style="list-style-type: none"> • Dumb • WYSE60 • VT100 • ANSI • TVI925 • IBM3151TE • VT320 (specifically supporting VT320-7) • HP700 (specifically supporting HP700/44) • Term1, Term2, Term3 (user-defined terminals) <p>Default: Dumb</p>
Require Login	<p>When users access the Terminal Server through the serial port, they must be authenticated using the local user database.</p> <p>Default: Enabled</p>
User Service Settings Button	<p>After a user has been successfully authenticated, the Terminal Server will connect to the specified host using the specified protocol according to:</p> <ul style="list-style-type: none"> • the User Service parameter for locally configured users • the Default User Service parameter for users who are externally authenticated <p>See User Service Settings for field descriptions of the various User Service Settings.</p>
Connect to Remote System	<p>When the serial port is started, the Terminal Server will initiate a connection to the specified host using the specified protocol. With this option, user authentication will not be performed by the Terminal Server.</p> <p>Default: Disabled</p>
Protocol	<p>Specify the protocol that will be used to connect to the specified host.</p> <p>Default: Telnet</p>
Settings Button	<p>Click this button to define the settings for the protocol that will be used to connect the user to the specified host.</p>
Host Name	<p>The name (resolvable via DNS) or IP address of the configured host the Terminal Server will connect to.</p>
TCP Port	<p>The TCP Port that the Terminal Server will use to connect to the host.</p> <p>Default: 23</p>
Automatically	<p>If the serial port hardware parameters have been setup to monitor DSR or DCD, the host session will be started once the signals are detected. If no hardware signals are being monitored, the Terminal Server will initiate the session immediately after being powered up.</p> <p>Default: Enabled</p>
When any data is received	<p>Initiates a connection to the specified host when any data is received on the serial port.</p> <p>Default: Disabled</p>

When *<hex value>* is received Initiates a connection to the specified host only when the specified character is received on the serial port.
Default: Disabled

Advanced Tab Field Descriptions

Configure the following parameters:

Enable Message of the Day (MOTD) Enables/disables the display of the message of the day.
Default: Disabled

Reset Terminal on disconnect When enabled, resets the terminal definition connected to the serial port when a user logs out.
Default: Disabled

Allow Port Locking When enabled, the user can lock his terminal with a password using the **Hotkey Prefix** (default Ctrl-a) **^a l** (lowercase L). The Terminal Server prompts the user for a password and a confirmation.
Default: Disabled

Hotkey Prefix	<p>The prefix that a user types to lock a serial port or redraw the Menu.</p> <p>Data Range:</p> <ul style="list-style-type: none"> • ^a l—(Lowercase L) Locks the serial port until the user unlocks it. The user is prompted for a password (any password, excluding spaces) and locks the serial port. Next, the user must retype the password to unlock the serial port. • ^r—When you switch from a session back to the Menu, the screen may not be redrawn correctly. If this happens, use this command to redraw it properly. This is always Ctrl R, regardless of the Hotkey Prefix. <p>You can use the Hotkey Prefix key to lock a serial port only when the Allow Port Locking parameter is enabled.</p> <p>Default: Hex 01 (Ctrl-a, ^a)</p>
Idle Timeout	<p>Use this timer to close a connection because of inactivity. When the Idle Timeout expires, the Terminal Server will end the connection.</p> <p>Default: 0 seconds so the port will never timeout</p> <p>Range: 0-4294967 seconds (about 49 days)</p>
Session Timeout	<p>Use this timer to forcibly close the session/connection when the Session Timeout expires.</p> <p>Default: 0 seconds so the port will never timeout</p> <p>Range: 0-4294967 seconds (about 49 days)</p>
Session Strings	<p>Controls the sending of ASCII strings to serial devices at session start as follows;</p> <ul style="list-style-type: none"> • Send at Start—If configured, this string will be sent to the serial device on power-up of the Terminal Server or when a kill line command is issued on this serial port. If the "monitor DSR" or "monitor DCD" options are set, the string will also be sent when the monitored signal is raised. Range: 0-127 alpha-numeric characters Range: hexadecimal 0-FF • Delay after Send—If configured, will inset a delay after the string is sent to the device. This delay can be used to provide the serial device with time to process the string before the session is initiated or terminated. Default: 10 ms
Dial Timeout	<p>The number of seconds the Terminal Server will wait to establish a connection to a remote modem.</p> <p>Range: 1-99</p> <p>Default: 45 seconds</p>
Dial Retry	<p>The number of times the Terminal Server will attempt to re-establish a connection with a remote modem.</p> <p>Range: 0-99</p> <p>Default: 2</p>
Dial In	<p>If the device is remote and will be dialing in via modem or ISDN TA, enable this parameter.</p> <p>Default: Disabled</p>
Dial Out	<p>If you want the modem to dial a number when the serial port is started, enable this parameter.</p> <p>Default: Disabled</p>

User Service Settings

Login Settings

These settings apply to users who are accessing the network from a terminal connected to the Terminal Server's serial port. The Telnet settings take effect when the connection method is defined in the user's profile.

Configure the following parameters:

- | | |
|---------------------------------|--|
| Limit Connection to User | Makes the serial port dedicated to the specified user. The user won't need to enter their login name - just their password. |
| Initial Mode | Specifies the initial interface a user navigates when logging into the serial port.
Data Options: Menu, Command Line
Default: Command Line |
| Terminal Pages | The number of video pages the terminal supports.
Range: 1-7
Default: 5 pages |

Telnet Settings

The Telnet settings apply when the **User Service** is set to **Telnet** or the Terminal profile specifies a **Telnet** connection to a host. When the Terminal Server initiates a Telnet connection to a host, it is acting as a Telnet client.

Configure the following parameters:

- | | |
|----------------------|---|
| Terminal Type | Type of terminal attached to this serial port; for example, ANSI or WYSE60. |
|----------------------|---|

Enable Local Echo	<p>Toggles between local echo of entered characters and suppressing local echo. Local echo is used for normal processing, while suppressing the echo is convenient for entering text that should not be displayed on the screen, such as passwords. This parameter can be used only when Enable Line Mode is enabled.</p> <p>Default: Disabled</p>
Enable Line Mode	<p>When enabled, keyboard input is not sent to the remote host until Enter is pressed, otherwise input is sent every time a key is pressed.</p> <p>Default: Disabled</p>
Map CR to CRLF	<p>When enabled, maps carriage returns (CR) to carriage return line feed (CRLF).</p> <p>Default: Disabled</p>
Interrupt	<p>Defines the interrupt character. Typing the interrupt character interrupts the current process. This value is in hexadecimal.</p> <p>Default: 3 (ASCII value ^C)</p>
Quit	<p>Defines the quit character. Typing the quit character closes and exits the current telnet session. This value is in hexadecimal.</p> <p>Default: 1c (ASCII value FS)</p>
EOF	<p>Defines the end-of-file character. When Enable Line Mode is enabled, entering the EOF character as the first character on a line sends the character to the remote host. This value is in hexadecimal.</p> <p>Default: 4 (ASCII value ^D)</p>
Erase	<p>Defines the erase character. When Line Mode is Off, typing the erase character erases one character. This value is in hexadecimal.</p> <p>Default: 8 (ASCII value ^H)</p>
Echo	<p>Defines the echo character. When Line Mode is On, typing the echo character echoes the text locally and sends only completed lines to the host. This value is in hexadecimal.</p> <p>Default: 5 (ASCII value ^E)</p>
Escape	<p>Defines the escape character. Returns you to the command line mode. This value is in hexadecimal.</p> <p>Default: 1d (ASCII value GS)</p>

Serial Tunneling Profile

Overview

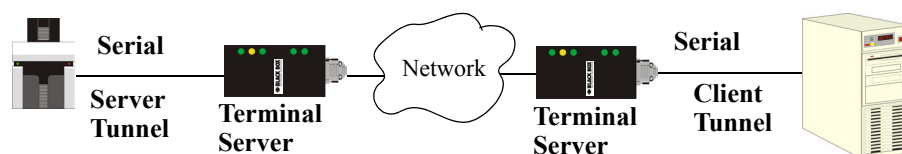
The Serial Tunneling profile allows two Terminal Servers to be connected back-to-back over the network to establish a virtual link between two serial ports based on RFC 2217.

Functionality

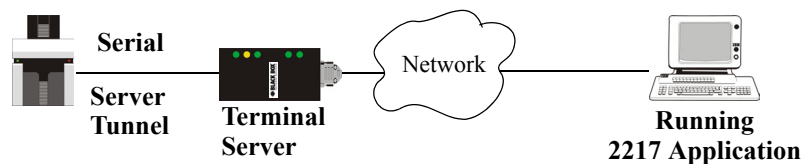
The serial device that initiates the connection is the **Tunnel Client** and the destination is the **Tunnel Server**, although once the serial communication tunnel has been successfully established, communication can go both ways.



A more detailed implementation of the Serial Tunneling profile is as follows:



The **Server Tunnel** will also support Telnet Com Port Control protocol as detailed in RFC 2217.



The Terminal Server serial port signals will also follow the signals on the other serial port. If one serial port receives DSR then it will raise DTR on the other serial port. If one serial port receives CTS then it will raise RTS on the other serial port. The CD signal is ignored.

General Tab Field Descriptions

Serial Tunneling Settings

A serial tunnel consists of two IOLANs connected over a TCP/IP network and creating a virtual link between two serial ports.

☒ **Act as Tunnel Server**

Listen for connections on:

TCP port:

☐ **Enable TCP Keepalive**

☐ **Act as Tunnel Client**

Establish connection to:

Host Name:

TCP Port:

Configure the following parameters:

Act As Tunnel Server	<p>The Terminal Server will listen for an incoming connection request on the specified Internet Address on the specified TCP Port.</p> <p>Default: Enabled</p>
TCP Port	<p>The TCP port that the Terminal Server will listen for incoming connection on.</p> <p>Default: 10000+serial port number; so serial port 2 is 10002.</p>
Enable TCP Keepalive	<p>Enables a per-connection TCP keepalive feature. After the configured number of seconds, the connection will send a gratuitous ACK to the network peer, thus either ensuring the connection stays active OR causing a dropped connection condition to be recognized.</p> <p>This parameter needs to be used in conjunction with Monitor Connection Status Interval parameter found in the Serial, Advanced, Advanced Settings tab. The interval determines how long the Terminal Server will wait during inactivity before "testing" the connection. It should be noted that if a network connection is accidentally dropped, it can take as long as the specified interval before anyone can reconnect to the serial port.</p> <p>Default: Disabled</p>
Act as Tunnel Client	<p>The Terminal Server will initiate the connection the Tunnel Server.</p> <p>Default: Disabled</p>
Host Name	<p>A preconfigured host name that is associated with the IP address of the Tunnel Server.</p>
TCP Port	<p>The TCP port that the Terminal Server will use to connect to the Tunnel Server.</p> <p>Default: 10000+serial port number; so serial port 5 is 10005.</p>

Advanced Tab Field Descriptions

The screenshot shows a configuration window titled 'Advanced Serial Tunneling Settings'. It has several tabs: General, Advanced (selected), Hardware, Email Alert, Packet Forwarding, and SSL/TLS. Inside the 'Advanced' tab, there are five input fields with labels: 'Break Length' (set to 1000), 'Delay After Break' (set to 0), 'Session Strings' (containing 'Send at Start' and 'Send at End' sub-fields), and 'Delay after Send' (set to 10). Each field is followed by the unit 'milliseconds'.

Configure the following parameters:

- | | |
|--------------------------|---|
| Break Length | The Terminal Server will initiate the connection the Tunnel Server.
Default: Disabled |
| Delay After Break | A preconfigured host name that is associated with the IP address of the Tunnel Server. |
| Session Strings | <p>Controls the sending of ASCII strings to serial devices at session start and session termination as follows;</p> <ul style="list-style-type: none"> ● Send at Start—If configured, this string will be sent to the serial device on power-up of the Terminal Server or when a kill line command is issued on this serial port. If the "monitor DSR" or "monitor DCD" options are set the string will also be sent when the monitored signal is raised.
Range: 0-127 alpha-numeric characters. Non printable ascii characters must be entered in this format <027>. The decimal numbers within the brackets must be 3 digits long (example 003 not 3). To enter the < (less than symbol) precede the symbol with a \ (backslash symbol). ● Send at End—If configured, this string will be sent to the serial device when the TCP session on the LAN is terminated. If multihost is configured, this string will only be sent to the serial device when the profile is configured as a listen mode connection and after all multihost connections are terminated. Non printable ascii characters must be entered in this format <027>.
Range: 0-127 alpha-numeric characters. The decimal numbers within the brackets must be 3 digits long (example 003 not 3). To enter the < (less than symbol) precede the symbol with a \ (backslash symbol). ● Delay after Send—If configured, a delay time is sent to the device. This delay can be used to provide the serial device with time to process the string before the session is initiated.
Range: 0-65535 ms
Default: 10 ms |

Virtual Modem Profile

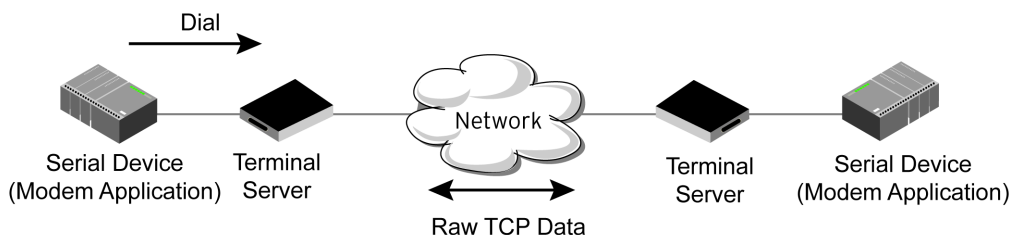
Overview

Virtual Modem (Vmodem) is a feature of the Terminal Server that provides a modem interface to a serial device. It will respond to AT commands and provide signals in the same way that a serially attached modem would. This feature is typically used when you are replacing dial-up modems with the Terminal Server in order to provide Ethernet network connectivity.

Functionality

The serial port will behave in exactly the same fashion as it would if it were connected to a modem. Using AT commands, it can configure the modem and the issue a dial-out request (ATDT). The Terminal Server will then translate the dial request into a TCP connection and data will begin to flow in both directions. The connection can be terminated by 'hanging' up the phone line.

You can also manually start a connection by typing **ATD<ip_address>,<port_number>** and end the connection by typing **+++ATH**. The **ip_address** can be in IPv4 or IPv6 formats and is the IP address of the receiver. For example, **ATD123.34.23.43,10001** or you can use **ATD12303402304310001**, without any punctuation (although you do need to add zeros where there are not three digits presents, so that the IP address is 12 digits long).



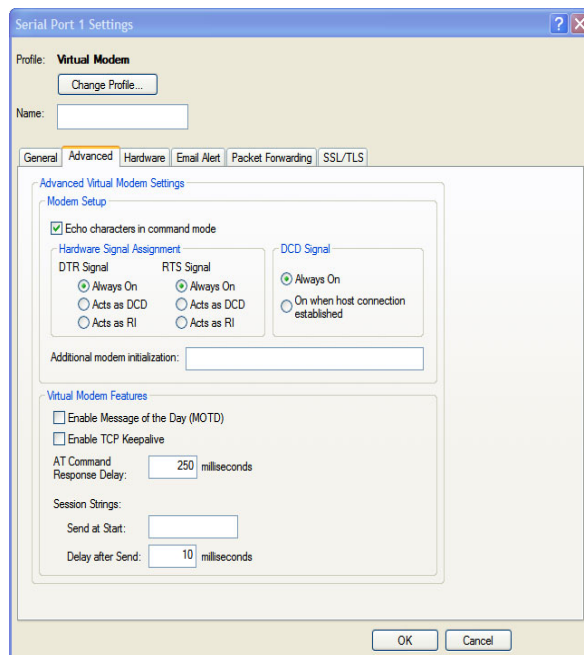
General Tab Field Descriptions

Configure the following parameters:

- Listen on TCP Port** The Terminal Server TCP port that the Terminal Server will listen on.
Default: 10000 + serial port number (for example, serial port 12 defaults to 10012)
- Connect Automatically At Startup** When enabled, automatically establishes the virtual modem connection when the serial port becomes active.
Default: Enabled
- Host Name** The preconfigured target host name.
- TCP Port** The port number the target host is listening on for messages.
Default: 0 (zero)
- Connect Manually Via AT Command** When enabled, the virtual modem requires an AT command before it establishes a connection. Specify this option when your modem application sends a phone number or other AT command to a modem. The serial device can supply an IP address directly or it can provide a phone number that will be translated into an IP address by the Terminal Server using the mapping table.
Default: Disabled
- Phone Number to Host Mapping Button** When your modem application provides a phone number in an AT command string, you can map that phone number to the destination host.
 See [Phone Number to Host Mapping](#) for information about the window that appears when you click this button.
- Send Connection Status As** When enabled, the connection success/failure indication strings are sent to the connected device, otherwise these indications are suppressed. This option also determines the format of the connection status results that are generated by the virtual modem.
Default: Enabled
- Verbose String** When enabled, the connection status is sent by text strings to the connected device.
Default: Disabled

Success String	String that is sent to the serial device when a connection succeeds. Default: CONNECT <speed>, for example, CONNECT 9600
Failure String	String that is sent to the serial device when a connection fails. Default: NO CARRIER
Numeric Codes	When enabled, the connection status is sent to the connected device using the following numeric codes: <ul style="list-style-type: none"> ● 0 OK ● 1 CONNECTED ● 2 RING ● 3 NO CARRIER ● 4 ERROR ● 6 INTERFACE DOWN ● 7 CONNECTION REFUSED ● 8 NO LISTNER Default: Enabled

Advanced Tab Field Descriptions



Configure the following parameters:

Echo characters in command mode	When enabled, echoes back characters that are typed in (equivalent to ATE0/ATE1 commands). Default: Disabled
DTR Signal Always On	Specify this option to make the DTR signal always act as a DTR signal. Default: Enabled
DTR Signal Acts as DCD	Specify this option to make the DTR signal always act as a DCD signal. Default: Disabled

DTR Signal Acts as RI	Specify this option to make the DTR signal always act as a RI signal. Default: Disabled
RTS Signal Always On	Specify this option to make the RTS signal always act as a RTS signal. Default: Enabled
RTS Signal Acts as DCD	Specify this option to make the RTS signal always act as a DCD signal. Default: Disabled
RTS Signal Acts as RI	Specify this option to make the RTS signal always act as a RI signal. Default: Disabled
DCD Signal Always on	When you configure the DTR or RTS signal pin to act as a DCD signal, enable this option to make the DCD signal stay on. Default: Enabled
DCD Signal On when host connection established	When you configure the DTR or RTS signal pin to act as a DCD signal, enable this option to make the DCD signal active only during active communication. Default: Disabled.
Additional modem initialization	<p>You can specify additional virtual modem commands that will affect how virtual modem starts. The following commands are supported: ATQn, ATVn, ATEn, ATS0, AT&Z1, AT&Sn, AT&Rn, AT&Cn, AT&F, ATS2, ATS12, and ATDS1.</p> <p>See Appendix A, <i>Virtual Modem AT Commands</i> for a more detailed explanation of the support initialization commands.</p>
Enable Message of the Day (MOTD)	When enabled, displays the Message of the Day (MOTD) when a successful virtual modem connection is made. Default: Disabled
Enable TCP Keepalive	<p>Enables a per-connection TCP keepalive feature. After the configured number of seconds, the connection will send a gratuitous ACK to the network peer, thus either ensuring the connection stays active OR causing a dropped connection condition to be recognized.</p> <p>This parameter needs to be used in conjunction with Monitor Connection Status Interval parameter found in the Serial, Advanced, Advanced Settings tab. The interval determines how long the Terminal Server will wait during inactivity before "testing" the connection. It should be noted that if a network connection is accidentally dropped, it can take as long as the specified interval before anyone can reconnect to the serial port.</p> <p>Default: Disabled</p>
AT Command Response Delay	<p>The amount of time, in milliseconds, before an AT response is sent to the requesting device.</p> <p>Default: 250 ms</p>

Session Strings

Controls the sending of ASCII strings to serial devices at session start as follows;

- **Send at Start**—If configured, this string will be sent to the serial device on power-up of the Terminal Server or when a kill line command is issued on this serial port. If the "monitor DSR" or "monitor DCD" options are set, the string will also be sent when the monitored signal is raised.

Range: 0-127 alpha-numeric characters

Range: hexadecimal 0-FF

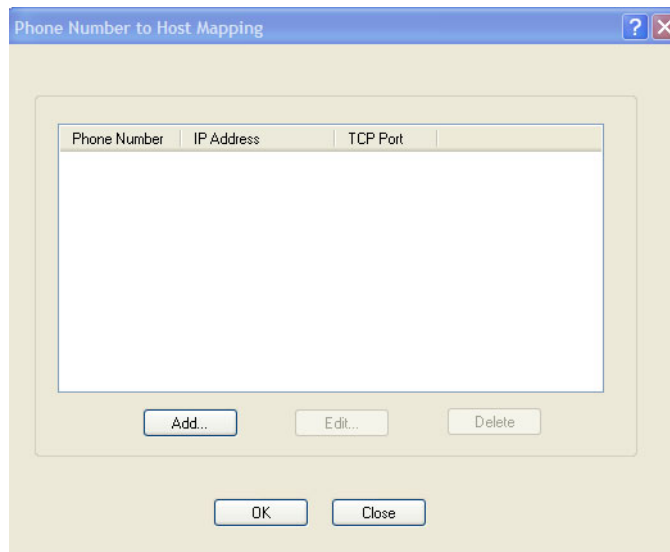
- **Delay after Send**—If configured, will inset a delay after the string is sent to the device. This delay can be used to provide the serial device with time to process the string before the session is initiated or terminated.

Default: 10 ms

Phone Number to Host Mapping

If your modem application dials using a phone number, you can add an entry in the Phone Number to Host Mapping window that can be accessed by all serial ports configured as Virtual Modem. You need to enter the phone number sent by your modem application and the Terminal Server IP address and TCP Port that will be receiving the 'call.' The Terminal Server supports up to 4 entries.

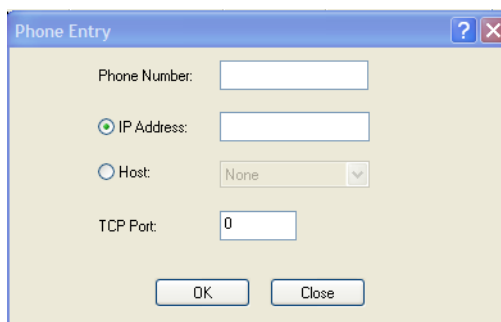
The following buttons are available:



- Add Button** Click the **Add** button to display a window that allows you to configure the phone number or AT command your modem application sends and the Terminal Server's IP address and TCP port number that is receiving the call.
- Edit Button** Click on a phone number entry and click the **Edit** button to change any values configured for the phone number.
- Delete Button** Click on a phone number entry and click the **Delete** button to remove it from the phone number list.

VModem Phone Number Entry

Create an entry in the Phone Number to Host Mapping window.



- Phone Number** Specify the phone number that your application uses to connect to the remote location. Note: The Terminal Server does not validate the phone number, so it must be entered in the exact way it is issued by the application. For example, if you enter 555-1212 in this table and the application sends 5551212, the Terminal Server will not match the two numbers. Spaces will be ignored.

Host IP Address	Specify the IP address of the remote host that is receiving the virtual modem connection.
Host Name	Select the host name (from the host table) of the Terminal Server that is receiving the virtual modem connection.
TCP Port	Specify the TCP port that the remote host is listening on for the vmodem connection. Default: 0

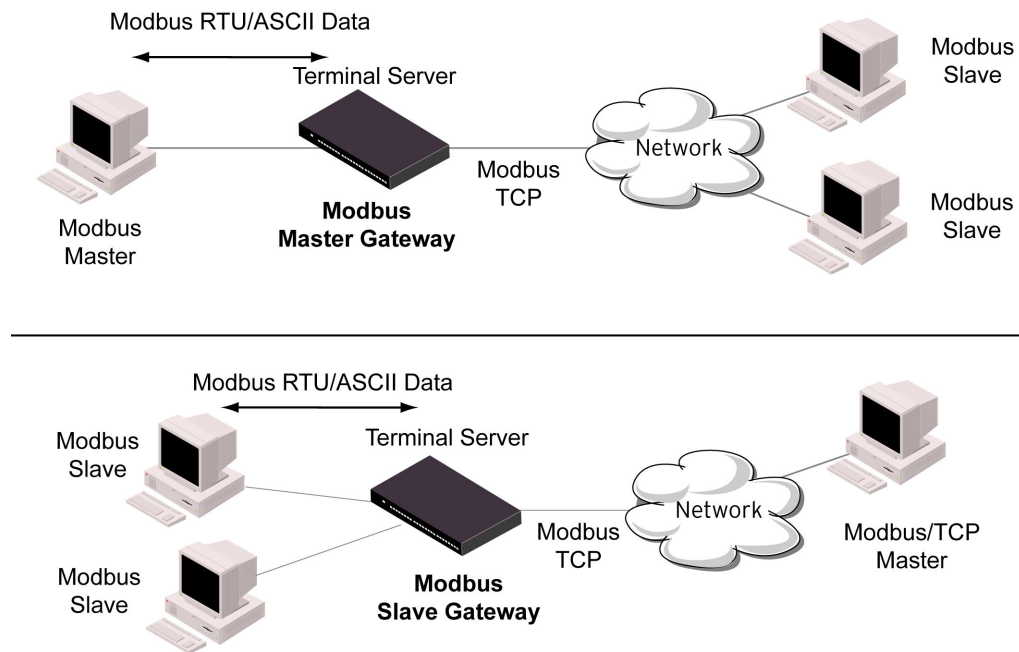
Modbus Gateway Profile

Overview

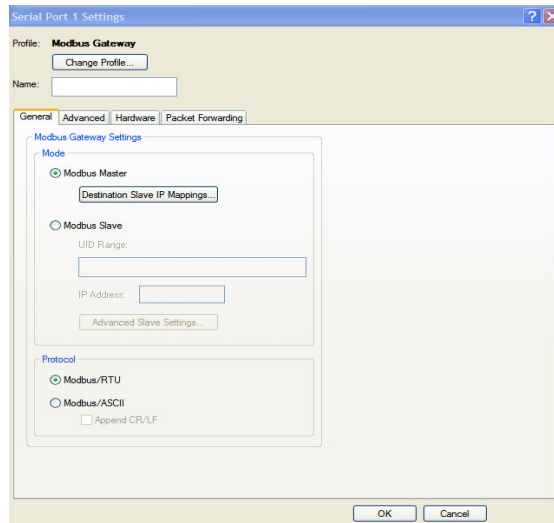
Each serial port can be configured as either a Modbus Master gateway or a Modbus Slave gateway, depending on your configuration and requirements.

Functionality

The Modbus Gateway profile configures a serial port to act as a Modbus Master Gateway or a Modbus Slave Gateway.



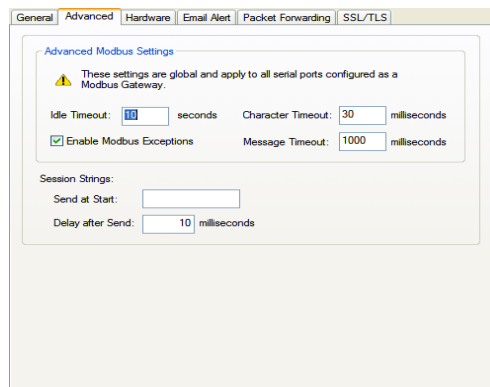
General Tab Field Descriptions



Configure the following parameters:

Mode	<p>Specify how the Modbus Gateway is defined on the serial port.</p> <p>Data Options:</p> <ul style="list-style-type: none"> • Modbus Master—Typically, the Modbus Master is connected to the Serial Port and is communicating to Modbus Slaves on the network. • Modbus Slave—Typically, the Modbus Master is accessing the Terminal Server through the network to communicate to Modbus Slaves connected to the Terminal Server's Serial Ports. <p>Default: Modbus Master Gateway</p>
Destination Slave IP Mappings Button	<p>Click this button to launch the Destination Slave IP Settings window, where you can configure the TCP/Ethernet Modbus Slaves that the Modbus Master on the Serial Port will communicate with.</p>
UID Range	<p>You can specify a range of UIDs (1-247), in addition to individual UIDs.</p> <p>Field Format: Comma delimited; for example, 2-35, 50, 100-103</p>
IP Address	<p>Set the IP address to be used for this serial port when using the IP Aliasing feature.</p> <p>See Enable IP Aliasing for details on how to enable this feature.</p>
Advanced Slave Settings Button	<p>Click this button to configure global Modbus Slave settings.</p>
Modbus/RTU	<p>Select this option when the Modbus/RTU protocol is being used for communication between the Modbus Master and Slave.</p> <p>Default: Enabled</p>
Modbus/ASCII	<p>Select this option when Modbus/ASCII protocol is being used for communication between the Modbus Master and Slave.</p> <p>Default: Disabled</p>
Append CR/LF	<p>When Modbus/ASCII is selected, adds a CR/LF to the end of the transmission; most Modbus devices require this option.</p> <p>Default: Enabled</p>

Advanced Field Descriptions

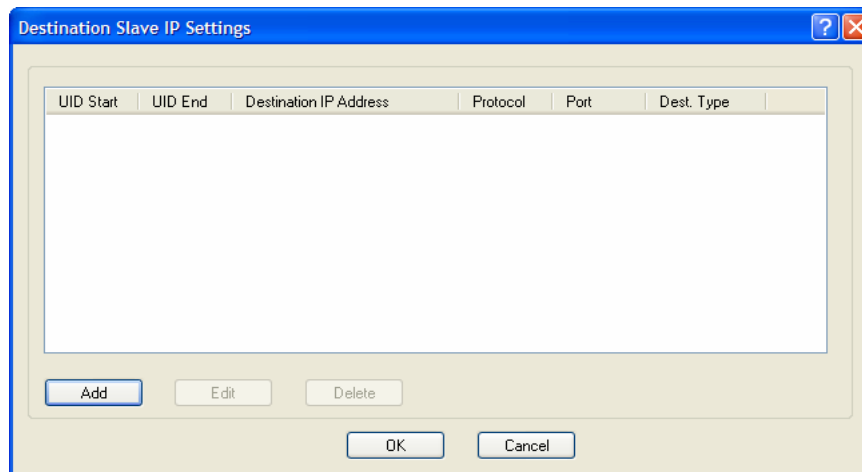


Configure the following parameters:

- | | |
|---------------------------------|---|
| Idle Timeout | <p>Use this timer to close a connection because of inactivity. When the Idle Timeout expires, the Terminal Server will end the connection.</p> <p>Range: 0-4294967 seconds (about 49 days)</p> <p>Default: 0 (zero), which does not timeout, so the connection is permanently open.</p> |
| Enable Modbus Exceptions | <p>Click this button to launch the Destination Slave IP Settings window, where you can configure the TCP/Ethernet Modbus Slaves that the Modbus Master on the Serial Port will communicate with.</p> |
| Character Timeout | <p>Used in conjunction with the Modbus RTU protocol, specifies how long to wait, in milliseconds, after a character to determine the end of frame.</p> <p>Range: 10-10000</p> <p>Default: 30 ms</p> |
| Message Timeout | <p>Time to wait, in milliseconds, for a response message from a Modbus TCP or serial slave (depending if the Modbus Gateway is a Master Gateway or Slave Gateway, respectively) before sending a Modbus exception.</p> <p>Range: 10-10000</p> <p>Default: 1000 ms</p> |
| Session Strings | <p>Controls the sending of ASCII strings to serial devices at session start as follows;</p> <ul style="list-style-type: none"> ● Send at Start—If configured, this string will be sent to the serial device on power-up of the Terminal Server or when a kill line command is issued on this serial port. If the "monitor DSR" or "monitor DCD" options are set, the string will also be sent when the monitored signal is raised. <p>Range: 0-127 alpha-numeric characters</p> <p>Range: hexadecimal 0-FF</p> ● Delay after Send—If configured, will inset a delay after the string is sent to the device. This delay can be used to provide the serial device with time to process the string before the session is initiated or terminated. <p>Default: 10 ms</p> |

Modbus Slave IP Settings Field Descriptions

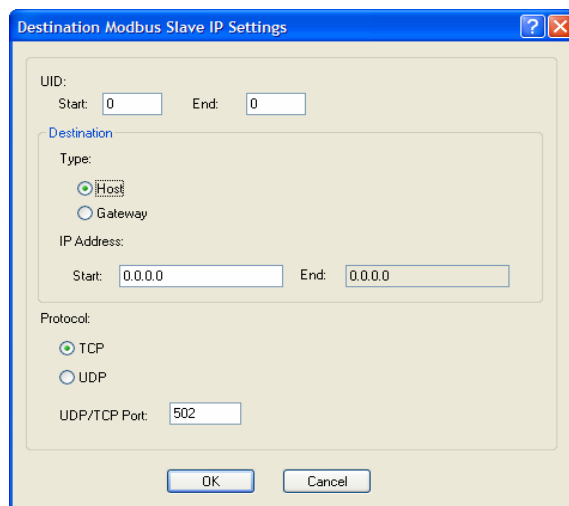
This window is used to configure the Modbus Slaves.



The following buttons are available:

- Add Button** Adds an entry into the Modbus Destination Slave IP Settings table.
- Edit Button** Edits an entry in the Modbus Destination Slave IP Settings table.
- Delete Button** Deletes an entry from the Modbus Destination Slave IP Settings table.

Adding/Editing Modbus Slave IP Settings



Configure the following parameters:

- UID Start** When **Destination** is set to **Host** and you have sequential Modbus Slave IP addresses (for example, 10.10.10.1, 10.10.10.2, 10.10.10.3, etc.), you can specify a UID range and the Terminal Server will automatically increment the last digit of the configured IP address. Therefore, you can specify a UID range of 1-100, and the Terminal Server will route Master Modbus messages to all Modbus Slaves with IP addresses of 10.10.10.1 - 10.10.10.100.
Range: 1-247
Default: 0 (zero)

UID End	<p>When Destination is set to Host and you have sequential Modbus Slave IP addresses (for example, 10.10.10.1, 10.10.10.2, 10.10.10.3, etc.), you can specify a UID range and the Terminal Server will automatically increment the last digit of the configured IP address. Therefore, you can specify a UID range of 1-100, and the Terminal Server will route Master Modbus messages to all Modbus Slaves with IP addresses of 10.10.10.1 - 10.10.10.100.</p> <p>Range: 1-247</p> <p>Default: 0 (zero)</p>
Type	<p>Specify the configuration of the Modbus Slaves on the network.</p> <p>Data Options:</p> <ul style="list-style-type: none">● Host—The IP address is used for the first UID specified in the range. The last octet in the IPv4 address is then incremented for subsequent UID's in that range. The Host option is not applicable for IPv6 addresses.● Gateway—The Modbus Master Gateway will use the same IP address when connecting to all the remote Modbus slaves in the specified UID range. <p>Default: Host</p>
Start IP Address	<p>The IP address of the TCP/Ethernet Modbus Slave.</p> <p>Field Format: IPv4 or IPv6 (IPv6 format not supported for Destination Host)</p>
End IP Address	<p>Displays the ending IP address of the TCP/Ethernet Modbus Slaves, based on the Start IP address and the UID range.</p>
Protocol	<p>Specify the protocol that is used between the Modbus Master and Modbus Slave(s).</p> <p>Data Options: TCP or UDP</p> <p>Default: TCP</p>
UDP/TCP Port	<p>The destination port of the remote Modbus TCP Slave that the Terminal Server will connect to.</p> <p>Range: 0-65535</p> <p>Default: 502</p>

Modbus Slave Advanced Settings Field Descriptions

Configure the following parameters:

TCP/UDP Port	The network port number that the Slave Gateway will listen on for both TCP and UDP messages. Default: 502
Next Request Delay	A delay, in milliseconds, to allow serial slave(s) to re-enable receivers before issuing next Modbus Master request. Range: 0-1000 Default: 50 ms
Enable Serial Modbus Broadcasts	When enabled, a UID of 0 (zero) indicates that the message will be broadcast to all Modbus Slaves. Default: Disabled
Request Queuing	When enabled, allows multiple, simultaneous messages to be queued and processed in order of reception. Default: Enabled
Embedded	When this option is selected, the address of the slave Modbus device is embedded in the message header. Default: Enabled
Remapped	Used for single device/port operation. Older Modbus devices may not include a UID in their transmission header. When this option is selected, you can specify the UID that will be inserted into the message header for the Modbus slave device. This feature supersedes the Broadcast feature. Default: Disabled
Remap UID	Specify the UID that will be inserted into the message header for the Slave Modbus serial device. Range: 1-247 Default: 1

- Enable IP Aliasing** When enabled, allows for multiple requests to serial slaves (from an Ethernet Master/s) to be processed simultaneously.
Default: Off
 See [IP Address](#) for details about setting the IP address to be used with this serial port.

Advanced

Advanced Serial Settings Tab

Overview

Advanced serial port settings apply to all serial ports.

Field Descriptions

The screenshot shows the 'Advanced Serial Settings' tab selected. It contains three sections: 'Advanced Serial Settings' with three unchecked checkboxes, 'Data Logging' with a 'Buffer Size' of 4 KB and an unchecked 'Pre V4.3 Mode' checkbox, and 'Monitor Connections' with 'Status Interval' of 180 seconds, 'Retry Interval' of 5 seconds, and 'Retry' of 5 Attempts.

Section	Field	Value	Unit/Label
Advanced Serial Settings	Process Break Signals	<input type="checkbox"/>	
	Flush Data Before Closing Serial Port	<input type="checkbox"/>	
	Deny Multiple Network Connections	<input type="checkbox"/>	
Data Logging	Buffer Size	4	KB
	Pre V4.3 Mode	<input type="checkbox"/>	
Monitor Connections	Status Interval	180	seconds
	Retry Interval	5	seconds
	Retry	5	Attempts

Configure the following parameters:

- Process Break Signals** Enables/disables proprietary inband SSH break signal processing and the Telnet break signal.
Default: Disabled
- Flush Data Before Closing Serial Port** When enabled, deletes any pending outbound data when a port is closed.
Default: Disabled

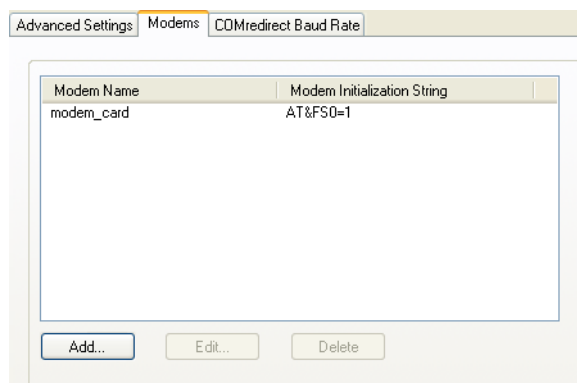
Deny Multiple Network Connections	<p>Allows only one network connection at a time per a serial port. Application accessing a serial port device across a network with get a connection (socket) refused until:</p> <ul style="list-style-type: none"> • All data from previous connections on that serial port has drained • There are no other connections • Up to a 1 second interconnection poll timer has expired <p>This also enables a per-connection TCP keepalive feature. After approximately 3 minutes of network connection idle time, the connection will send a gratuitous ACK to the network peer, thus either ensuring the connection stays active OR causing a dropped connection condition to be recognized by all peer network connections.</p> <p>Applications using this feature need to be aware that there can be some considerable delay between a network disconnection and the port being available for the next connection attempt, allowing any data sent on prior connections to be transmitted out of the serial port. Application network retry logic needs to accommodate this feature.</p> <p>Default: Disabled</p>
Pre V4.3G Data Logging Mode	Enable previous data logging pre V4.3G firmware.
Data Logging Buffer Size	<p>The minimum data buffer size is 1 KB for all models. The maximum data buffer size is 2000 KB for the TS1, all other models are 4000 KB. If the data buffer is filled, incoming serial data will overwrite the oldest data.</p> <p>Values: 1-2000 KB (TS1) default 4 KB</p> <p>Values: 1-4000 KB (all other models) default 256 KB</p>
Monitor Connection Interval Status	<p>Specify how often, in seconds, the Terminal Server will send a TCP Keepalive to services that support TCP Keepalive.</p> <p>Default: 180 seconds</p>
Retry Interval	<p>Set the maximum time to wait for a response after sending a TCP keepalive message. messages.</p> <p>Values: 1-32767 seconds</p> <p>Default: 5 seconds</p>
Retry Attempts	<p>The number of TCP keepalive retries before the connection is closed.</p> <p>Values: 1-32767</p> <p>Default: 5</p>

Modems Tab

Overview

You need to configure a modem if there is a modem connected to the Terminal Server.

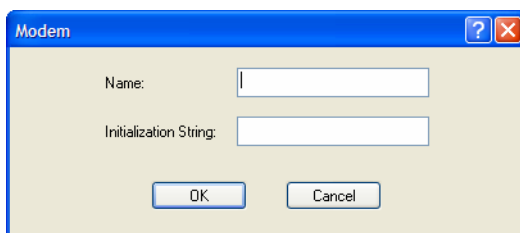
When you click on the **Modems** tab, you will see the following:



If any modems have been configured, they will be displayed.

Adding/Editing a Modem

You can add new modems or edit existing modems through the following window:



Configure the following parameters:

Name The name of the modem.
Restrictions: Do not use spaces.

Initialization String The initialization string of the modem; see your modem's documentation.

COMredirect Baud Rate Tab

Overview

The COMredirect utility acts as a COM port redirector that allows applications to talk to serial devices across a network as though the serial devices were directly attached to the server.

Functionality

Since some older applications may not support the higher baud rates that the Terminal Server is capable of achieving, the baud rate can be mapped to a different value on the Terminal Server. Through COMredirect, you can map the baud rate of the host COM port to a higher baud rate for the serial line that connects the serial device and the Terminal Server. See [COMredirect](#) for more information about the COMredirect utility.

Field Definitions

COMredirect Baud	Actual Baud Rate
50	57600
75	75
110	115200
134	230400
150	150
200	200
300	300
600	600
1200	1200
1800	1800
2400	2400
4800	4800
9600	9600
19200	19200
38400	38400

Configure the following parameter:

Actual Baud Rate The actual baud rate that runs between the Terminal Server and the connected serial device. You can also specify a custom baud rate.

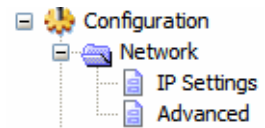
Range: 50 - 230400

7 Network Settings

Introduction

The Network section is used to configure the parameters that identify the Terminal Server within the network and how the Terminal Server accesses hosts on the network. The following configuration windows are available:

- **IP Settings**—This window sets up Terminal Server's name, IPv4 address, IPv6 address, and Ethernet information. See [IP Settings](#) for more information.
- **Advanced**—This window configures hosts that the Terminal Server will be communicating with and routes. See [Advanced](#) for more information on these options.



IP Settings

IPv4 Settings

Overview

The parameters in IPv4 settings are used to access the Terminal Server and are how the Terminal Server accesses the network.

Field Descriptions

The screenshot shows the 'IPv4 Settings' window with three tabs: 'IPv4 Settings', 'IPv6 Settings', and 'Advanced'. The 'IPv4 Settings' tab is active. It contains two sections: 'System Settings' and 'Ethernet Interface Settings'. In 'System Settings', the 'System Name' is set to 'localhost' and the 'Domain' is empty. In 'Ethernet Interface Settings', the 'Obtain IP address automatically using DHCP/BOOTP' option is selected. Below this, the 'Use the following IP address:' section shows 'IP Address' as '0 . 0 . 0 . 0' and 'Subnet Mask' as '0 . 0 . 0 . 0'. The 'Default Gateway' field is empty.

Configure the following parameters:

- | | |
|---|--|
| System Name | The System Name is used for informational purposes by such tools as the DeviceManager and is also used in conjunction with the Domain field to construct a fully qualified domain name (FQDN).
Default: localhost |
| Domain | This field is combined with the System Name to construct the fully qualified domain name (FQDN). For example, if the domain is mycompany.com and the Server Name is set to accounting , the FQDN would be accounting.mycompany.com . |
| Obtain IP Address automatically using DHCP/BOOTP | When enabled, the Terminal Server will request an IP address from the DHCP/BOOTP server. By default, when this option is enabled, the Terminal Server will also attempt to retrieve the DNS server, WINS server, and default gateway from the DHCP/BOOTP server.
Default: Disabled |
| Use the following IP Address | Assign a specific IP address to the Terminal Server. |
| IP Address | The Terminal Server's unique IPv4 network IP address. If you are using the Terminal Server in an IPv6 network, this field can be left blank.
Field Options: IPv4 address |
| Subnet Mask | The network subnet mask. For example, 255.255.0.0. |
| Default Gateway | Specify the gateway IP address that will provide general access beyond the local network.
Field Options: IPv4 address |

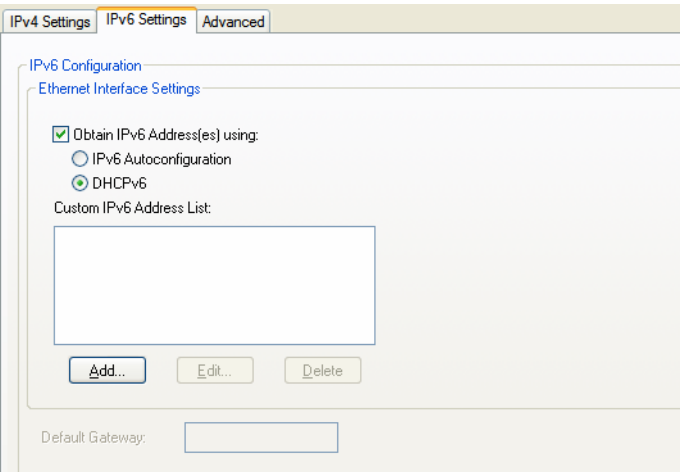
Default Gateway Obtain Automatically	When DHCP/BOOTP is enabled, you can enable this option to have the Terminal Server receive the Default Gateway IP address from the DHCP/BOOTP server. Default: Enabled
---	--

IPv6 Settings

Overview

The parameters in IPv6 settings are used to access the Terminal Server and are how the Terminal Server accesses the network.

Field Descriptions



Configure the following parameters:

Obtain IPv6 Address(es) using	When enabled, you can configure the Terminal Server to obtain the IPv6 address(es) using IPv6 Autoconfiguration or a DHCPv6 server. Default: Enabled
IPv6 Autoconfiguration	When enabled, the Terminal Server will send out a Router Solicitation message. If a Router Advertisement message is received, the Terminal Server will configure the IPv6 address(es) and configuration parameters based on the information contained in the advertisement. If no Router Advertisement message is received, the Terminal Server will attempt to connect to a DHCPv6 server to obtain IPv6 addresses and other configuration parameters. Default: Enabled
DHCPv6	When enabled, requests IPv6 address(es) and configuration information from the DHCPv6 server. Default: Disabled
Custom IPv6 List	Displays the list of custom configured IPv6 addresses.
Add Button	Adds a custom IPv6 address.
Edit Button	Edits an existing IPv6 address.
Delete Button	Deletes an IPv6 address from the Custom IPv6 address list.

Default Gateway	Specify the gateway IP address that will provide general access beyond the local network. Field Format: IPv6 address
DHCPv6 Settings IPv6 Address(es)	When enabled, the Terminal Server will accept IPv6 address(es) from the DHCPv6 server. Default: Disabled
DHCPv6 Settings Network Prefix	When enabled, the Terminal Server will accept the network prefix from the DHCPv6 server. Default: Disabled

Adding/Editing a Custom IPv6 Address

You can manually add one of the following:

- The IPv6 network prefix (and the Terminal Server will determine an IPv6 address based on the network prefix and the Terminal Server MAC address).
- The complete IPv6 address.

Field Descriptions

Configure the following parameters:

Create a unique IPv6 address on the network	When enabled, the Terminal Server will derive an IPv6 address from the entered network prefix and the Terminal Server's MAC address. Default: Enabled
Network Prefix	Specify the IPv6 network prefix. The Terminal Server will derive the complete IPv6 address from the entered network prefix and the Terminal Server's MAC address. Default: Enabled
Network Prefix IPv6 Prefix Bits	Specify the network prefix bits for the IPv6 address. Range: 0-64 Default: 64
Use the following IPv6 address	Enable this option when you want to enter a specific IPv6 address. Default: Disabled
IPv6 Address	Specify the complete IPv6 address. Field Format: IPv6 address

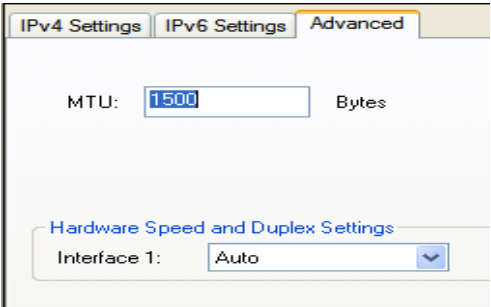
IPv6 Address IPv6 Prefix Bits Specify the network prefix bits for the IPv6 address.
Range: 0-128
Default: 64

Advanced

Overview

The **Advanced** tab configures the Ethernet interface hardware speed and duplex.

Field Descriptions



Configure the following parameter:

- Ethernet1 Speed and Duplex**

Define the Ethernet connection speed.
Data Options:
 - **Auto**—automatically detects the Ethernet interface speed and duplex
 - **10 Mbps Half Duplex**
 - **10 Mbps Full Duplex**
 - **100 Mbps Half Duplex**
 - **100 Mbps Full Duplex****Default:** Auto
- Maximum Transmission Unit**

The Maximum Transmission Unit (MTU) size of an IP frame that will be sent over the network. Only one MTU size can be set for both IPV4 and IPV6 frames.
Default: 68-1500 bytes
Default: 68-1500 bytes

Advanced

Host Table

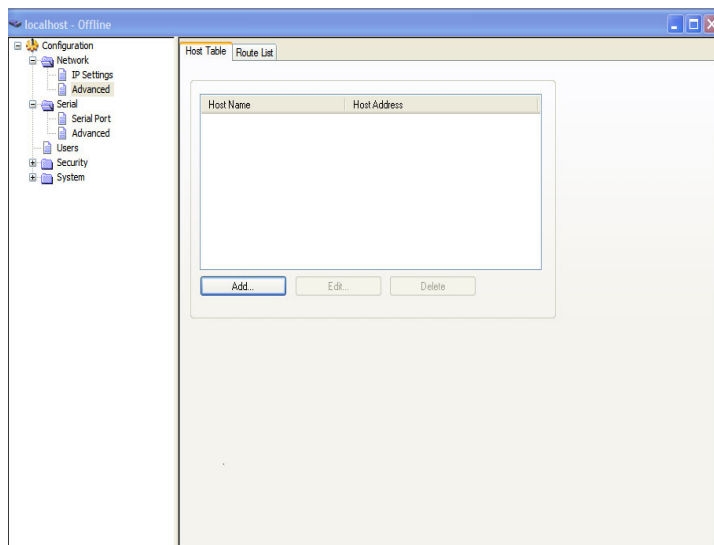
Overview

The Host table contains the list of hosts that will be accessed by an IP address from the Terminal Server. This table will contain a symbolic name for the host as well as its IP address. When a host entry is required elsewhere in the configuration, the symbolic name will be used.

Functionality

You can configure up to 50 hosts using IPv4 or IPv6 internet addresses on desktop Terminal Server models.

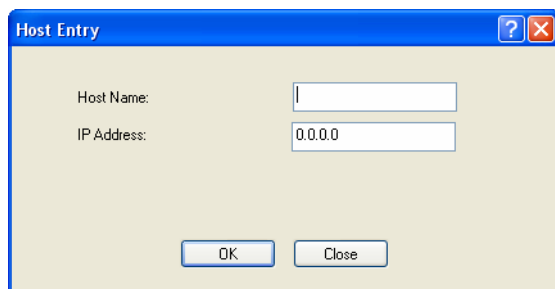
Field Descriptions



Configure the appropriate parameters:

- Add Button** Adds a host to the host table.
- Edit Button** Changes a host that already exists in the host table.
- Delete Button** Deletes a host from the host table.

Adding/Editing a Host



Configure the appropriate parameters:

- Host Name** The name of the host. This is used only for the Terminal Server configuration.
Text Characteristics: Up to 14 characters, no spaces.
- IP Address** The host's IP address.
Text Characteristics: IPv4 or IPv6 Address

Route List

Overview

Entering routes in the routing list enables the identification of gateways to be used for accessing specific hosts or external networks from the Terminal Server's local network.

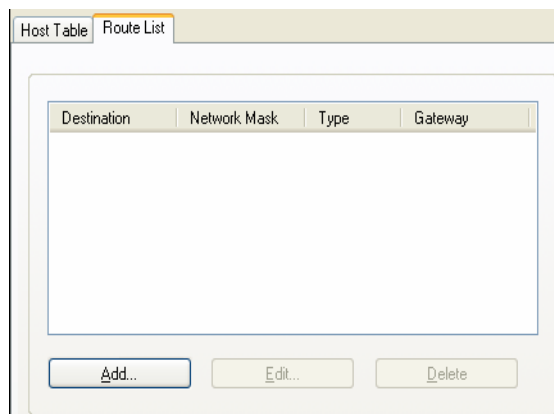
Functionality

There are three types of routes:

- **Default**—A route that provides general access beyond your local network.
- **Host**—A route defined for accessing a specific host external to your local network.
- **Network**—A route defined for accessing a specific network external to your local network.

You can specify up to 20 routes on desktop Terminal Server models.

Field Descriptions



The following buttons are available:

- Add Button** Adds a route to the Route List.
- Edit Button** Changes an existing route in the Route List.
- Delete Button** Deletes a route from the Route List.

Adding/Editing Routes

From the **Route List** tab, if you click the **Add** or **Edit** button, you will be able to add a new or edit an existing route.

Configure the appropriate parameters:

Type	<p>Specify the type of route you want to configure.</p> <p>Data Options:</p> <ul style="list-style-type: none"> ● Host—A route defined for accessing a specific host external to your local network. ● Network—A route defined for accessing a specific network external to your local network. ● Default—A route which provides general access beyond your local network. <p>Default: Default</p>
IP Address	<p>When the route Type is defined as Host, this field will contain the IP address of the host. If the route Type is defined as Network, the network portion of the IP address must be specified and the Host port of the address will be set to 0. Example: to access network 10.10.20, the address 10.10.20.0 would be specified in this field.</p> <p>Format: IPv4 or IPv6 Address</p>
IPv4 Subnet Mask	<p>When the route is a Network route, you must specify the network's subnet mask.</p>
IPv6 Prefix Bits	<p>If the IP address is IPv6, then you must specify the network's prefix bits.</p> <p>Range: 0-128</p>
Host	<p>The host that is being used at the route gateway.</p>

8

Configuring Users

Introduction

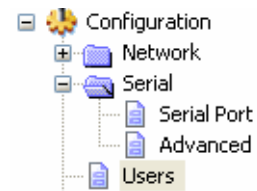
You can configure up to four users in the Terminal Server's local user database, in addition to the Admin user. A user can even represent a device, like a barcode reader or a card swipe device, that you want to be authenticated.

When users are connecting to the Terminal Server via serial ports, the user database can be used to:

- Have the user authenticated prior to establishing a connection to a network host.
- Establish a different connection type to the host specific to each user.
- Create a profile different from the Default user profile.

When users are connecting to the Terminal Server from a network connection, the user database can be used to:

- Authenticate users prior to providing access to a serially attached console port (such as a Unix server or router).



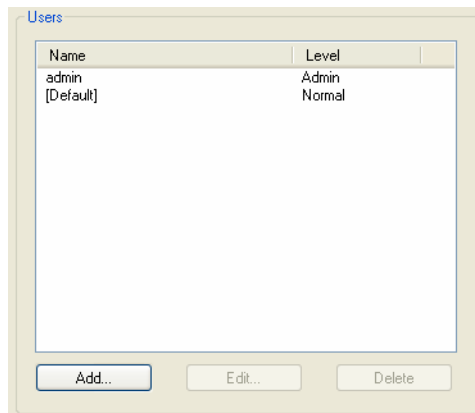
User Settings

Overview

The Users window allows you to add, edit, and delete users from the Terminal Server. **Note:** you can not delete the **admin** user.

Functionality

The Users window displays the users who have been configured. You can add users, edit existing users, or delete users from this window. See [Adding/Editing Users](#) for information on the parameters available when adding or editing a user.



Adding/Editing Users

General Tab

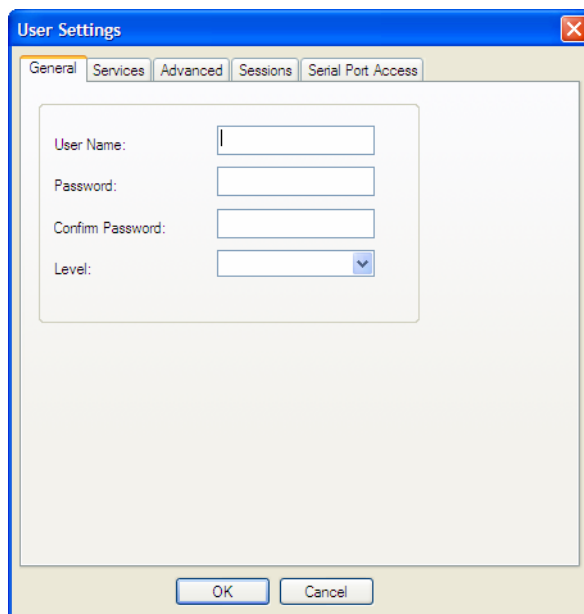
Overview

The General tab configures the basic user information.

Functionality

You must, minimally, provide a **User Name** and **Level** for a user.

Field Descriptions

The image shows a screenshot of a 'User Settings' dialog box. The dialog has a blue title bar with a close button (X) in the top right corner. Below the title bar is a tabbed interface with five tabs: 'General' (selected), 'Services', 'Advanced', 'Sessions', and 'Serial Port Access'. The 'General' tab contains four input fields: 'User Name:' (a text box), 'Password:' (a text box), 'Confirm Password:' (a text box), and 'Level:' (a dropdown menu). At the bottom of the dialog are two buttons: 'OK' and 'Cancel'.

Configure the following parameters:

- | | |
|-------------------------|---|
| User Name | The name of the user.
Restrictions: Do not use spaces. |
| Password | The password the user will need to enter to login to the Terminal Server. |
| Confirm Password | Enter the user's password again to verify it is entered correctly. |

Level

The access that a user is allowed.

Data Options:

- **Admin**—The admin level user has total access to the Terminal Server. You can create more than one admin user account but we recommend that you only have one. They can monitor and configure the Terminal Server. Users configured with this level can access the unit either via serial Terminal Profile connection or via a network originated Telnet connection to the Terminal Server.
- **Normal**—The Normal level user has limited access to the Terminal Server. Limited CLI commands and Menu access are available with the ability to configure the user's own configuration settings. Users configured with this level can access the unit either via serial Terminal Profile connection or via a network originated Telnet connection to the Terminal Server.
- **Restricted**—The Restricted level user can only access predefined sessions or access the Easy Port Access menu. Users configured with this level will be restricted to pre-defined sessions or limited CLI commands when connecting through the serial port via the Terminal Profile. The CLI commands are limited to those used for initiating a session. If connection to the Terminal Server is done with Telnet from the network, the user will be presented with the Easy Port Access menu.
- **Menu**—The menu level user will only be able to access predefined session when connecting through a serial port with the Terminal profile or will be limited to the Easy Port Access menu when connecting from the network. The Easy Port Access allows the user to connect to the accessible line without disconnecting their initial connection to the Terminal Server. Does not have any access to CLI commands.

When the Admin user logs into the Terminal Server, the prompt ends with a #, whereas all other users' prompts ends with a \$ or £, depending on the character set.

Default: Normal

Note: A technique for giving a serially attach user (dial-in or terminal attached), the same menus as one that is network connected is to do the following:

1. Define the serial port with a Terminal Profile using telnet protocol with a direct connection to Host IP address 127.0.0.0 (local loop back).
2. When the user connects to that serial port a Telnet session will be established to the Terminal Server and the user will appear to have connected from the network.

Services Tab

Overview

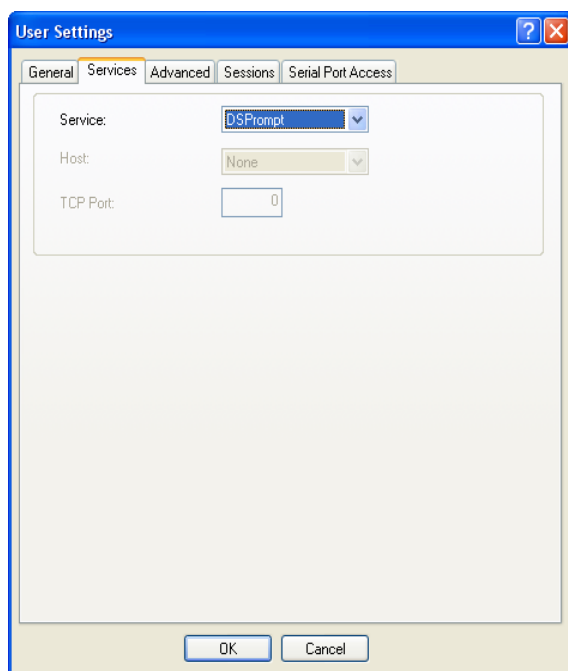
The Services tab configures the connection parameters for a user. Any connection parameters configured in this window will override the serial port connection parameters.

Functionality

When a **Terminal** profile is set for the serial port and **Require Login** has been selected, user's accessing the Terminal Server through the serial port will be authenticated. Once authentication is successful, the Terminal Server will start a Telnet connection to the specified **Host IP/TCP Port**.

Within the **Terminal** profile, there are a number of settings that apply to possible **Services**. Once it is known which user is connected, and which service is to be used, then the settings from both the **Terminal** profile and the user are used. User parameters take precedence over serial port parameters.

Field Descriptions



Configure the following parameters:

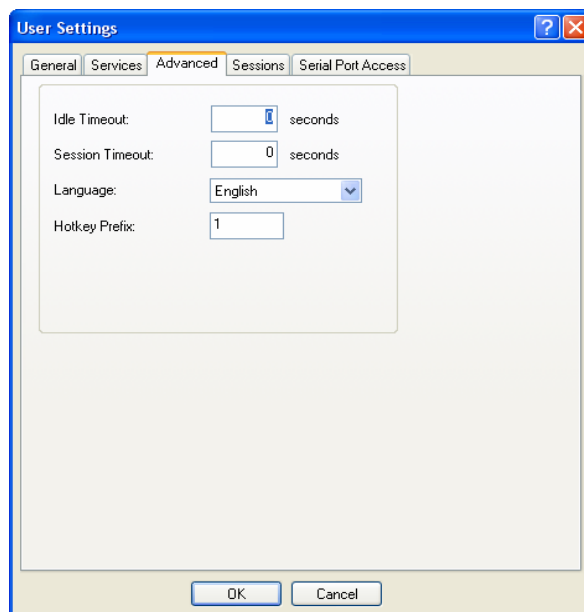
Service	Used in conjunction with the Terminal Profile . After the user has successfully been authenticated, the specified service is started. Data Options: DSPrompt, Telnet, TCP Clear Default: DSPrompt
Host IP	When the User Service is Telnet , this is the target host name or IP address. If no IP address or host name is specified, the Host IP value in the Default User configuration will be used. Default: 0.0.0.0.
TCP Port	When the User Service is Telnet , this is the target port number. The default value will change based on the type of Service selected; the most common known port numbers are used as the default values.

Advanced Tab

Overview

The **Advanced** tab is used to configure those parameters that control the user session; this includes session length, language, the hotkey used for switching between sessions.

Field Descriptions



Configure the following parameters:

- | | |
|------------------------|---|
| Idle Timeout | <p>The amount of time, in seconds, before the Terminal Server closes a connection due to inactivity. The default value is 0 (zero), meaning that the Idle Timer will not expire (the connection is open permanently). The User Idle Timeout will override all other Serial Port Idle Timeout parameters.</p> <p>Range: 0-4294967</p> <p>Default: 0</p> |
| Session Timeout | <p>The amount of time, in seconds, before the Terminal Server forcibly closes a user's session (connection). The default value is 0 (zero), meaning that the session timer will not expire (the session is open permanently, or until the user logs out). The User Session Timeout will override all other Serial Port Session Timeout parameters.</p> <p>Range: 0-4294967</p> <p>Default: 0</p> |
| Language | <p>You can specify whether a user will use English or Custom Language as the language that appears in the Menu, CLI, or WebManager. The Terminal Server supports one custom language that must be downloaded to the Terminal Server.</p> <p>Default: English</p> <p>See Language Support for more information about Custom Languages.</p> |

Hotkey Prefix

The prefix that a user types to control the current session.

Data Options:

- **^a number**—To switch from one session to another, press **^a** (Ctrl-a) and then the required session number. For example, **^a 2** would switch you to session 2. Pressing **^a 0** will return you to the Terminal Server Menu.
- **^a n**—Display the next session. The current session will remain active. The lowest numbered active session will be displayed.
- **^a p**—Display the previous session. The current session will remain active. The highest numbered active session will be displayed.
- **^a m**—To exit a session and return to the Terminal Server. You will be returned to the menu. The session will be left running.
- **^a l**—(Lowercase L) Locks the serial port until the user unlocks it. The user is prompted for a password (any password, excluding spaces) and the serial port is locked. The user must retype the password to unlock the serial port.
- **^r**—When you switch from a session back to the Menu, the screen may not be redrawn correctly. If this happens, use this command to redraw it properly. This is always **Ctrl R**, regardless of the **Hotkey Prefix**.

The **User Hotkey Prefix** value overrides the **Serial Port Hotkey Prefix** value. You can use the **Hotkey Prefix** keys to lock a serial port only when the serial port's **Allow Port Locking** parameter is enabled.

Default: Hex 01 (Ctrl-a or ^a)

Sessions Tab

Overview

The Sessions tab is used to configure specific connections for users who are accessing the network through the Terminal Server's serial port.

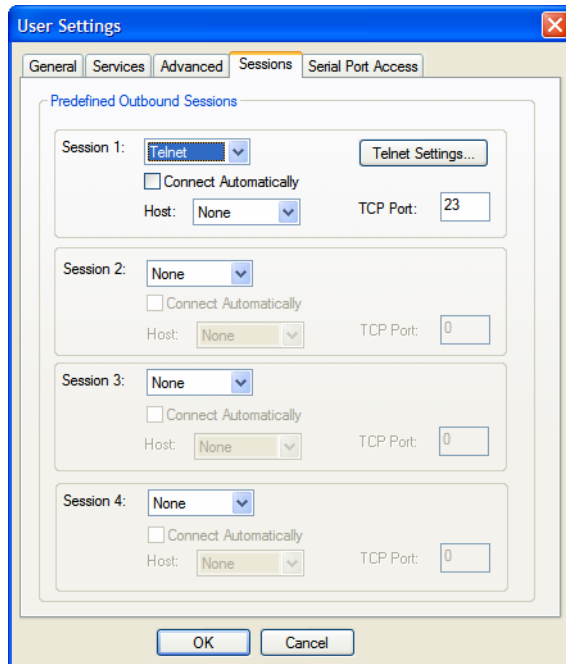
Functionality

Users who have successfully logged into the Terminal Server (**User Service** set to **DSprompt**) can start up to four login sessions on network hosts. These users start sessions through the Easy Port Menu option **Sessions**.

Multiple sessions can be run simultaneously to the same host or to different hosts. Users can switch between different sessions and also between sessions and the Terminal Server using **Hotkey** commands (see [Hotkey Prefix](#) for a list of commands).

Users with **Admin** or **Normal** privileges can define new sessions and use them to connect to Network hosts; they can even configure them to start automatically on login to the Terminal Server. **Restricted** and **Menu** users can only start sessions predefined for them in their user configuration.

Field Descriptions



Configure the following parameters:

Session 1, 2, 3, 4 You can configure up to four (4) sessions that the user can select from to connect to a specific host after that user has successfully logged into the Terminal Server (used only on serial ports configured for the **Terminal** profile).

Data Options:

- **None**—No connection is configured for this session.
- **Telnet**—For information on the Telnet connection window, see [Telnet Settings](#).

Default: None

Settings Button Click this button to configure the connection parameters for this session.

Connect Automatically Specify whether or not the session(s) will start automatically when the user logs into the Terminal Server.

Default: Disabled

Host The host that the user will connect to in this predefined session.

Default: None

TCP Port The TCP port that the Terminal Server will use to connect to the host in this predefined session.

Default: 23

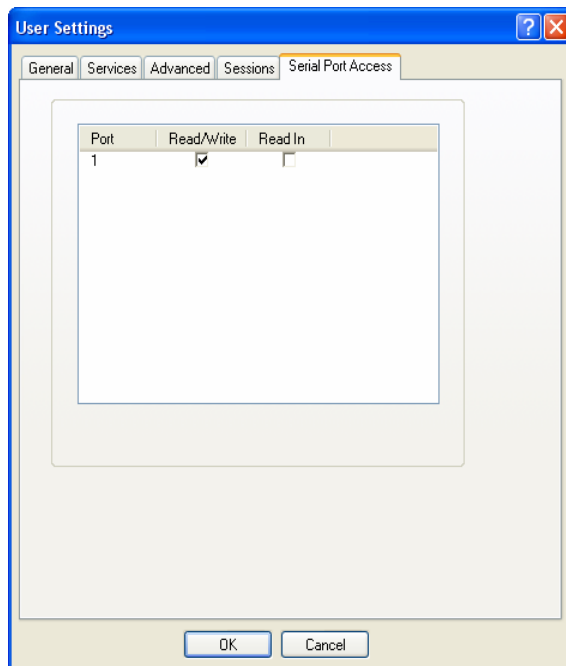
Serial Port Access Tab

Overview

The **Serial Port Access** tab controls the user's read/write access on any given Terminal Server serial port. This pertains to users that are connecting from the network to a serial device over a Console Management type session.

This can be useful when you have multiple users connecting to the same serial device and you wish to control the viewing and/or the write to and from the device. See the **User Authentication** parameters in the *Console Management Profile* for the serial port settings.

Field Descriptions



Configure the following parameters:

Serial Port Access Specifies the user access rights to each Terminal Server serial port device. There can be multiple users connected to a particular serial device and these settings determine the rights of this user for any of the listed serial ports.

Data Options:

- **Read/Write**—The user has read and write access to the serial port.
- **Read In**—The User will see data going to the serial port, from all network-connected users that have write privileges to this serial port.
- **Read Out**—The user will have access to all data originating from the serial device.

Users can read data going in both directions by selecting both the **Read In** and **Read Out** options.

Default: Read/Write

9

Configuring Security

Introduction

The **Security** group includes the following configuration options:

- **Services**—This configuration window is used to enable/disable client and daemon services that run in the Terminal Server. See [Services](#) for more information.



Services

Overview

Services are either daemon or client processes that run on the Terminal Server. You can disable any of the services for security reasons.

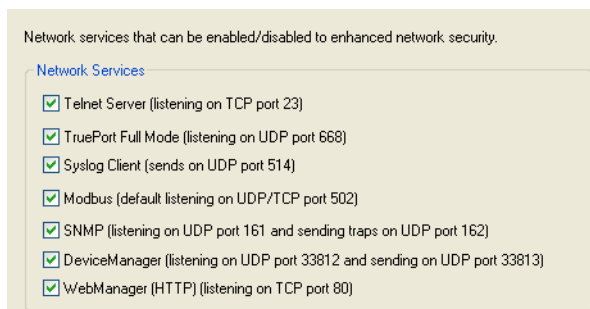
Functionality

If you disable any of the daemons, it can affect how the Terminal Server can be used or accessed. For example, if you disable the WebManager service, you will not be able to access the Terminal Server with the WebManager. If you disable the DeviceManager service, the DeviceManager will not be able to connect to the Terminal Server. If you do not want to allow users to Telnet to the Terminal Server, you can disable the Telnet Server service; therefore, disabling daemons can also be used as an added security method for accessing the Terminal Server.

By default, all daemon and client applications are enabled and running on the Terminal Server.

Field Descriptions

Enable/disable the following options:



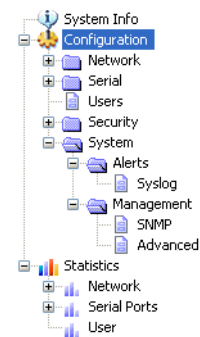
Telnet Server	Telnet daemon process in the Terminal Server listening on TCP port 23.
COMredirect Full Mode	The COMredirect daemon process in the Terminal Server that supports COMredirect Full Mode on UDP port 668. You can still communicate with the Terminal Server in Light Mode when this service is disabled.
Syslog Client	Syslog client process in the Terminal Server.
Modbus	Modbus daemon process in the Terminal Server listening on port 502.
SNMP	SNMP daemon process in the Terminal Server listening on port 161.
DeviceManager	DeviceManager daemon process in the Terminal Server. If you disable this service, you will not be able to connect to the Terminal Server with the DeviceManager application. The DeviceManager listens on port 33812 and sends on port 33813.
WebManager (HTTP)	WebManager daemon process in the Terminal Server listening on port 80.

Note: TCP ports 2601, 2602 and 2603 are used internally by the Terminal Server.

10 Configuring the System

Introduction

This chapter describes the alerts (syslog) that can be configured for the Terminal Server and the advanced options (SNMP and other miscellaneous configuration options) that you will want to look at to see if they are required for your implementation.



Alerts

Syslog

Overview

The Terminal Server can be configured to send system log messages to a syslog daemon running on a remote host if the **Syslog** service is activated. You can configure a primary and secondary host for the syslog information and specify the level for which you want syslog information sent.

Note: You must ensure that the **Syslog Client** service in the **Security, Services** window is enabled (by default it is enabled) for these settings to work.

Field Descriptions

Syslog

Level

(Send More)

- Debug
- Info
- Notice
- Warning
- Error
- Critical
- Alert
- Emergency

(Send Less)

Primary Host: None

Secondary Host: None

Configure the following parameters:

Primary Host

The first preconfigured host that the Terminal Server will attempt to send system log messages to; messages will be displayed on the host's monitor.

Default: None

Secondary Host	If the Terminal Server cannot communicate with the primary host, then the Terminal Server will attempt to send system log messages to this preconfigured host; messages will be displayed on the host's monitor. Default: None
Level	Choose the event level that triggers a syslog entry. Data Options: Emergency, Alert, Critical, Error, Warning, Notice, Info, Debug Default: Emergency

Management

SNMP

Overview

If you are using SNMP to manage/configure the Terminal Server, or to view statistics or traps, you must set up a User in SNMP version 3 or a Community in SNMP version 1,2 to allow your SNMP manager to connect to the Terminal Server; this can be done in the DeviceManager, WebManager, CLI, or Menu. You must then load the **blackbox-ds.MIB** (found on the CD-ROM packaged with the Terminal Server) file into your SNMP manager before you connect to the Terminal Server.

Note: Ensure that the **SNMP** service found in the **Security, Services** page is enabled (by default it is enabled).

Field Descriptions

Configure the following parameters:

Contact	The name and contract information of the person who manages this SMNP node.
Location	The physical location of the SNMP node.

- Community** The name of the group that devices and management stations running SNMP belong to. This only applies to SNMP version 1 and version 2c.
- Internet Address** The IP address of the SNMP manager that will send requests to the Terminal Server. If the address is 0.0.0.0, any SNMP manager with the **Community** name can access the Terminal Server. If you specify a network address, for example 172.16.0.0, any SNMP manager within the local network with the **Community** name can access the Terminal Server.
Field Format: IPv4 or IPv6 address
- Permissions** Permits the Terminal Server to respond to SNMP requests.
Data Options:
- **None**—There is no response to requests from SNMP.
 - **Readonly**—Responds only to Read requests from SNMP.
 - **Readwrite**—Responds to both Read and Write requests from SNMP.
- Default:** None
- Read-Write User** Specified user can view and edit SNMP variables.
- Read-Only User** Specified user can only view SNMP variables.

Field Descriptions

The screenshot shows the 'SNMP Traps' configuration window. At the top, there are tabs for 'SNMP' and 'Traps'. The 'Traps' tab is active. Below the tabs, there is a section titled 'SNMP Traps' containing a table with columns: 'Internet Address', 'Version', 'Type', and 'Community (V1 or V2c)'. There are four rows in the table, each with a checkbox in the first column and the value '0.0.0.0' in the 'Internet Address' column. The 'Version' column has a dropdown menu set to 'v1', and the 'Type' column has a dropdown menu set to 'Trap'. The 'Community' column is empty. Below the table, there are two sections: 'Users (Version 3)' and 'Inform'. The 'Users (Version 3)' section has a 'User:' label and an empty text box. The 'Inform' section has 'Timeout:' and 'Retries:' labels with text boxes containing the values '1' and '3' respectively. At the bottom, there is a section titled 'Engine ID (Version 3)' with an 'Engine ID:' label and a text box containing 'Not Available'. Below this, there are two radio buttons: 'Use Default Engine ID' (which is selected) and 'Create Engine ID Using String' (which is unselected). To the right of the 'Create Engine ID Using String' radio button is an empty text box.

Configure the following parameters:

- Trap Checkbox** Check this box to enable the entry of the trap information.
- Internet Address** Defines the hosts (by IP address) that will receive trap messages generated by the Terminal Server. Up to four trap hosts can be defined.
Field Format: IPv4 or IPv6 address
- Version** Select the version of trap you want the Terminal Server to send. Valid options are v1, v2c or v3.
- Type** Select between Trap and Inform. Inform requires the host receiving the trap to acknowledge the receipt of the trap.

Community	The name of the group that devices and management stations running SNMP belong to. This only applies to SNMP version 1 and version 2c.
Timeout	This is only used for the Inform traps. Select the number of seconds to wait for the acknowledgement of the trap. Default: 1 second
Retries	This is only used for Inform traps. Select the number of times the trap will be sent if no acknowledgement is received. Default: 3
V3 Engine ID	This is the current Engine ID. The Engine ID is a string which uniquely identifies this SNMP agent.
V3 Use Default EngineID	When this field is selected, the firmware will use the default Engine ID. The default Engine ID uses the MAC address of the Ethernet interface to ensure that the Engine ID is unique to this agent.
V3 Create EngineID Using String	The string entered in this field will be combined with the defined string in hex of 800007AE04 to form the EngineID. Ensure each string is unique for each Terminal Server on your network.

Advanced

Overview

Review the configuration options in the Advanced page to determine if any of them apply to your implementation.

Login Tab Field Descriptions

Configure the following parameters:

Use System Name in Prompts	Displays the System Name field value instead of default product name. When enabled, the Server Name is displayed in the Terminal Server login prompt, CLI prompt, WebManager login screen, and the heading of the Menu. Default: Disabled
Display Login Banner	This parameter concerns the banner information (product name/software version). This banner information is presented to a user with a login prompt. For security reasons, you can turn off the display of this information. Default: Disabled

Use Custom Login Prompt	<p>When set, and a custom language file is in use, the login prompt will use the string defined in the language file as the login prompt instead of the default prompt, login:.</p> <p>Default: Disabled</p>
Bypass Login Password	<p>When set, authorized users who do not have a password set, with the exception of the Admin user, WILL NOT be prompted for a password at login with Local Authentication.</p> <p>Default: Disabled</p>
Use a Generic WebManager Login Screen	<p>When set, and the user connects to the Terminal Server using WebManager, the WebManager login screen that is displayed is generic — the Terminal Server banner, and firmware version are not displayed to the user.</p> <p>Default: Disabled</p>
Password Retry Limit	<p>The number of attempts a user is allowed to enter a password for a serial port connection from the network, before the connection is terminated and the user has to attempt to login again. For users logging into the serial port, if this limit is exceeded, the serial port is disabled for 5 minutes. A user with Admin level rights can restart the serial port, bypassing the timeout, by issuing a kill on the disabled serial port.</p> <p>Default: 3</p>
EasyPort Web	<p>Select Java if communication via port 23(Telnet) or port 22(SSH) is not restricted by a firewall.</p> <p>Select Javascript if you need to communicate through a firewall on port 8080 using EasyPort Web</p> <p>To end and close a Telnet session, type CTRL] then type quit</p> <p>To end and close a SSH session, on a new line type ~ . (period)..</p>

Bootup Files Tab Field Descriptions

You must have a TFTP server running on any host that you are uploading or downloading files to/from. When you specify the file path, the path must be relative to the default path set in your TFTP server software.

The screenshot shows a web interface with four tabs: Login, Bootup Files (selected), Message of the Day (MOTD), and TFTP. The Bootup Files tab contains two sections. The first section, titled 'Firmware', has 'Host:' and 'File:' labels followed by text input fields. The second section, titled 'Configuration', also has 'Host:' and 'File:' labels followed by text input fields.

Configure the following parameters:

Firmware Host	<p>The host name or IP address of the server that contains the firmware file. If you use a host name, it must exist in the Terminal Server's host table or be resolved by DNS.</p> <p>Field Format: Resolvable host name, IPv4 address, IPv6 address</p>
----------------------	---

- Firmware File** The path and file name, relative to the default path of your TFTP server software, of the update software for the Terminal Server that will be loaded when the Terminal Server is rebooted.
- Configuration Host** The host name or IP address of the server that contains the configuration file. If you use a host name, it must exist in the Terminal Server's host table or be resolved by DNS.
Field Format: Resolvable host name, IPv4 address, IPv6 address
- Configuration File** The path and file name, relative to the default path of your TFTP server software, of the configuration file for the Terminal Server that will be loaded when the Terminal Server is rebooted.

Message of the Day (MOTD) Tab Field Descriptions

The message of the day is displayed when users log into the Terminal Server through a telnet or SSH session or through WebManager or EasyPort Web.

There are two ways to retrieve the message of the day to be displayed to users when they log into the Terminal Server:

- The message of the day file is retrieved from a TFTP server every time a user logs into the Terminal Server. You must have a TFTP server running on any host that you are uploading or downloading files to/from when using TFTP. When you specify the file path, the path must be relative to the default path set in your TFTP server software.
- The message of the day file is downloaded to the Terminal Server and retrieved locally every time a user logs into the Terminal Server. You can download a MOTD file to the Terminal Server in the DeviceManager by selecting **Tools, Advanced, Custom Files** and then selecting the **Download Other File** option and browse to the MOTD file. In WebManager, select **Administration, Custom Files** and select the **Other File** option and browse to the MOTD file. After the MOTD is downloaded to the Terminal Server, you must specify the MOTD file name in the **Filename** field to access it as the message of the day (no **TFTP Host** parameter is required when the file is internal).

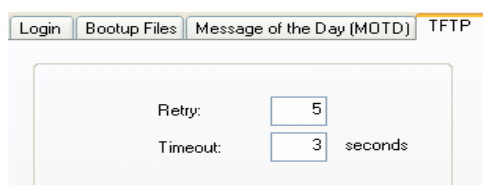
Configure the following parameters:

- TFTP Host** The host that the Terminal Server will be getting the Message of the Day file from.
Field Format: Resolvable host name, IPv4 address, IPv6 address
- Filename** The path and file name, relative to the default path of your TFTP server software, of the file that contains a string that is displayed when a user connects to the Terminal Server. The Terminal Server will look for the file internally (it must already be downloaded), if only the file is specified (no TFTP host) or the file cannot be found on the specified TFTP host.
- Display MOTD in WebManager/EasyPort Web** When enabled, displays the Message of the Day to users who are logging into WebManager or EasyPort Web.
Default: Disabled

TFTP Tab Field Descriptions

You must have a TFTP server running on any host that you are uploading or downloading files to/from.

Note: TFTP file transfers send via UDP packets. When the packet delivery is interrupted for any reason and a timeout occurs, that packet is resent if the retry count allows it. Therefore, if a very large file is being transferred and is interrupted, the entire file is not resent, just the part of the file that was not received.



The screenshot shows a web interface with four tabs: 'Login', 'Bootup Files', 'Message of the Day (MOTD)', and 'TFTP'. The 'TFTP' tab is active. Inside the tab, there is a light gray box containing two labels: 'Retry:' and 'Timeout:'. Next to 'Retry:' is a text input field containing the number '5'. Next to 'Timeout:' is a text input field containing the number '3', followed by the text 'seconds'.

Configure the following parameters:

- | | |
|----------------|--|
| Retry | The number of times the Terminal Server will retry to transmit a TPFT packet to/from a host when no response is received. A value of 0 (zero) means that the Terminal Server will not attempt a retry should TFTP fail.
Range: 0-5
Default: 5 |
| Timeout | The time, in seconds, that the Terminal Server will wait for a successful transmit or receipt of TFTP packets before retrying a TFTP transfer.
Range: 3-10
Default: 3 seconds |

11 System Administration

Introduction

This chapter addresses the functions that the Admin user or a user with Admin Level privileges might do. This chapter uses the DeviceManager as the configuration method described in most administrative functions. As a general rule, administrative functions are accessed from the menu bar in the DeviceManager and under the **Administration** option in the WebManager's navigation tree.

Managing Configuration Files

Saving Configuration Files

When you connect to the Terminal Server using either DeviceManager or WebManager, the Terminal Server's active configuration file is loaded into the configurator. To save a backup of the configuration file locally, do the following:

- In DeviceManager, select **File, Save As** from the menu bar. Notice that you can save the file as either a **.dme** or a **.txt** file. Either file format can be imported into the DeviceManager and downloaded to the Terminal Server in the future. The **.dme** is a binary file and the **.txt** file is a text file that can be viewed in any text editor.
- In WebManager, select under the **Administration** option, select **Backup/Restore**. Click the **Backup** button.

Downloading Configuration Files

You can download a configuration file to the Terminal Server by doing the following:

- In DeviceManager:
 1. Connect to the Terminal Server to retrieve the current configuration file.
 2. Open the configuration file you want to download to the Terminal Server by selecting **File, Import Configuration from a File** and then browsing to the configuration file. This will replace the retrieved configuration file.
 3. Select **Tools, Download Configuration to Terminal Server** or click the **Download All Changes** button.
 4. Reboot the Terminal Server.
- In WebManager:
 1. Under the **Administration** option, select **Backup/Restore**.
 2. Browse to the configuration file that you want to download to the Terminal Server.
 3. Click the **Restore** button.
 4. Reboot the Terminal Server.

Downloading Configuration Files to Multiple Terminal Servers

You can download a configuration file to multiple Terminal Servers at the same time by doing the following in DeviceManager (DeviceManager is the only configurator that does this function):

1. Select **Tools, Download Configuration to Multiple** Terminal Servers.
2. Specify the Terminal Servers that you want to download the configuration to:

Enter the following information for each Terminal Server that you want to configure with the same configuration file:

- | | |
|----------------------|---|
| IP Address | Enter the IP address of the Terminal Server that you want to download the configuration to.
Field Format: IPv4 or IPv6 address |
| Server Name | The name of the Terminal Server. The Terminal Server name that you put in this field is passed into the configuration before it is downloaded to the Terminal Server and cannot be left blank. |
| Password | Enter the Admin user password for the Terminal Server. |
| Reboot Server | Determines whether or not the Terminal Server is rebooted after it has received the new configuration. The new configuration definitions will not go into effect until the Terminal Server is rebooted. |

3. Click **Add** to add the Terminal Server to the download list. You can also click on a Terminal Server and edit any information and then click **Update** to make the edits permanent.
4. Click the **Download>** button to start the download process. A status window will display with the configuration download status.

Uploading Configuration Files

When you upload a configuration to the DeviceManager, you are uploading the Terminal Server's working configuration file. In most other configurators (the exception being SNMP), you are always seeing the working configuration file.

In DeviceManager, select **Tools, Upload Configuration from** Terminal Server. The working configuration file will automatically be loaded into the DeviceManager.

Specifying a Custom Factory Default Configuration

When you receive the Terminal Server, it comes with a factory default configuration that it can be reset to at any time. Administrators might find it useful to customize the factory default configuration file, so that if the Terminal Server gets reset to its factory defaults, it will be reset to defaults that the Administrator specified.

There are two ways you can set the custom factory default configuration:

- **Download a file to the Terminal Server**—You can download a custom factory default file to the Terminal Server using any of the configuration methods. In DeviceManager, you must connect to the Terminal Server and then select **Tools, Advanced, Custom Files, Custom Factory Default Configuration** and then specify the file. In WebManager, you must connect to the Terminal Server and then select **Administration, Reset, Factory Defaults, Set Current Configuration as Factory Default**.
- **Download the current configuration to the Terminal Server**—You can specify the configuration that you are working with/on as the custom factory default configuration using any of the configuration methods (you must be connected to the Terminal Server). In DeviceManager, select **Tools, Advanced, Set Factory Default to Terminal Server**. In WebManager, select **Administration, Reset, Factory Defaults, Get and Set Factory Default Configuration File**.

Resetting to the Original Factory Default Configuration

When you press the Reset button on the Terminal Server, the following take place:

- **Less than 3 seconds**—Reboots the Terminal Server.
- **Between 3 and 10 seconds**—Reboots the Terminal Server and resets the configuration to the factory default (either the original default configuration or the custom default configuration).
- **Over 10 seconds**—Reboots the Terminal Server and resets the configuration to the original factory default configuration.

Downloading Terminal Server Firmware

To upgrade the Terminal Server firmware (software):

- In DeviceManager, select **Tools, Advanced, Download Firmware** to Terminal Server. You can browse to the firmware location. Once the firmware download is complete, you will be prompted to reboot the Terminal Server. You can choose to reboot the Terminal Server at another time by selecting **Tools, Reset, Reboot** Terminal Server.
- In WebManager, under the **Administration** option, select **Update Firmware**. Either browse to the firmware file and then click the **Upload** button or configure the TFTP server and click the **Upload** button. Note: If you use the TFTP option, the specified TFTP server must be on the same subnet as the Terminal Server.

Upgrading the firmware does not affect the Terminal Server's configuration file or downloaded custom files.

Setting the Terminal Server's Date and Time

When you set the Terminal Server's time, the connection method and time zone settings can affect the actual internal clock time that is being set. For example, if you are connecting to the Terminal Server through the DeviceManager and your PC's time zone is set to Pacific Standard Time (GMT -8:00) and the Terminal Server's time zone is set to Eastern Standard Time (GMT -5:00), the Terminal Server's time is actually three hours ahead of your PC's time. Therefore, if you set the Terminal Server's time to 2:30 pm in the DeviceManager, the Terminal Server's actual internal clock time is 5:30 pm. This is the only configuration method that interprets the time and converts it between time zones, as necessary.

All other configuration methods set the Terminal Server's internal clock time to the time specified, with no interpretation.

To set the Terminal Server's system clock in DeviceManager, select **Tools, Advanced, Set Unit Time/Date**. The Set Date/Time window is displayed.

Note: Terminal Server models do not retain the date/time settings when the unit is rebooted.

Configure the following parameters:

Date	The Terminal Server's date. The format of the Terminal Server's date is dependent on the Windows operating system and regional settings.
Time	The Terminal Server's internal clock time, based on your PC's time zone. For example, if your PC's time zone is set to Pacific Standard Time (GMT -8:00) and the Terminal Server's time zone is set to Eastern Standard Time (GMT -5:00), the Terminal Server's time is three hours ahead of your PC's time. If you set the Terminal Server's time to 2:30 pm, the Terminal Server's actual internal clock time is 5:30 pm.
Use the PCs Date/Time	When enabled, sets the Terminal Server's time to the PCs time. Default: Enabled This option is unique to the DeviceManager.

Rebooting the Terminal Server

When you download any file (configuration, keys, certificates, firmware, etc.) to the Terminal Server, you must reboot the Terminal Server for it to take effect by selecting **Tools, Reset, Reboot Server** in DeviceManager and **Administration, Reboot Unit** in WebManager.

Resetting the serial port statistics

You can reset the serial port statistics back to zero.

Resetting the Terminal Server to Factory Defaults

You can reset the Terminal Server to its factory default configuration by selecting **Tools, Reset, Reset to Factory Default** in DeviceManager and **Administration, Reset, Factory Defaults** in WebManager. The Terminal Server will automatically reboot itself with the factory or custom factory default configuration.

Language Support

Two language files, in addition to English, are supplied on the supplemental CD, French and German. You can use any of these language files to create a translation into a language of your choice. You can download the language file (whether the language is supplied or translated) into the Terminal Server and select the **Language** option of **Custom Language** or **Customlang** (custom language), making the Menu and CLI field labels display in the desired language.

You can view Menu or CLI in one other language only (as well as English). If you download another language file, this new language will replace the first language you downloaded.

You can revert to English at any time; the English language is stored permanently in the Terminal Server and is not overwritten by your new language. Each user logged into the Terminal Server can operate in either English or the downloaded language.

Loading a Supplied Language

This section describes how to download a language file using the CLI, since it is the least intuitive method. French and German language files are provided on the supplemental CD.

To load one of the supplied languages into the Terminal Server, so the Menu or CLI fields appear in another language, do the following:

1. Open the supplemental CD and identify the language file, either **bb_ds_French.txt** or **bb_ds_German.txt**, or supply one of your own translated files.
2. Copy the language file to a host machine on the network; place it in the main file system or on the main hard drive.
3. Either use the TFTP defaults in the Terminal Server or, configure as necessary, TFTP in the Terminal Server.
4. In the CLI of the Terminal Server, enter the host IP address and file name; for example,

```
netload customlang 172.16.4.1 /temp/bb_ds_French.txt
```

The Terminal Server will download the language file via TFTP.

In DeviceManager select **Tools, Advanced, Custom Files** and then select **Download Custom Language File** and browse to the language file. In WebManager select **Administration, Custom Files** and then specify the **Custom Language File** option and browse to the language file.

5. To set an individual user to the new language, go to the **Users** menu and, in the **Language** field select **Customlang**. In the CLI (only) you can set individual users or all users to the new language; see the **set user *** command.

6. The user will see the change of language when he/she logs out (**Main Menu**, **Sessions Menu**, **Logout**) and logs back into the Terminal Server. If, as Admin user, you change your language setting to **Customlang**, you will see the text menus display in the new language when you save and exit the **Change User** form. Users with **Level Normal** can also change their display language.

Note: If you download a new software version, you can continue to use your language unchanged; however, we recommend translating the new strings, which will be added to the end of the language file. A **Reset to Factory Defaults** will reload the **Customlang** as English.

On successful download, the **Customlang** in the Terminal Server will be overwritten by the new language.

Translation Guidance

To help you with your translation, of supplied ASCII text language files we offer the following guidance:

- The Terminal Server will support languages other than English (and the supplied German and French languages). The English language file, **english.txt**, displays the character length of each line at the beginning of the line. If a translated line goes over that character length, it will be displayed truncated in the Menu or CLI.
- Translate line for line, do not omit lines if you do not know the translation; leave the original untranslated text in place. Also, you must maintain the same sequential order of lines. It is a good practice to translate the file using a text editor that displays line numbers, so you can periodically verify that the line sequence has not changed from the original file (by comparing it to the original file).
- Keep all translations in quotes, otherwise the line will not display properly.
- Each line must end with a carriage return.
- If a line contains only numbers, for example 38400, leave that line in place, unchanged (unless you are using a different alphabet).

Software Upgrades and Language Files

If you receive a software upgrade for the Terminal Server, the language files supplied on the supplemental diskette/CD might also have been updated. We will endeavour to provide a list of those changes in another text file on the same supplemental CD.

Note: The upgrade of your software (firmware) will not change the display of the language in the Menu or CLI.

If you are already using one of the supplied languages, French or German, you probably want to update the language file in the Terminal Server. Until you update the Terminal Server with the new language file, new text strings will appear in English.

If you are already using a language translated from an earlier version, you probably want to amend your translation. When a language file is updated, we will try to maintain the following convention:

1. New text strings will be added to the bottom of the file (not inserted into the body of the existing file).
2. Existing text strings, if altered, will be altered in sequence; that is, in their current position in the file.
3. The existing sequence of lines will be unchanged.
4. Until you have the changes translated, new text strings will appear in the Menu or CLI in English.

Downloading Terminal Definitions

All terminal types can be used on the Terminal Server. Some terminal types which are not already defined in the Terminal Server, however, are unable to use Full Screen mode (menus) and may not be able to page through sessions properly. When installed, the Terminal Server has several defined terminal types—Dumb, WYSE60, VT100, ANSI, TVI925, IBM3151, VT320-7, and HP700/44.

If you are not using, or cannot emulate, any of these terminal types, you can add up to three additional terminal definitions to the Terminal Server. The terminal definitions can be downloaded from a TCP/IP host.

To download terminal definitions, follow these steps:

1. Decide which TCP/IP host you are going to use. It must be a machine with enabled.
2. Configure TFTP in the Terminal Server as necessary.
3. Select **Tools, Advanced, Custom Files** from the menu bar.
4. From the **File Type** drop-down, select **Download Terminal Definition**. Select the terminal definition option **1, 2, or 3** and then browse to the terminal definition file that is being downloaded to the Terminal Server.
5. In the **Terminal** profile, select the **Terminal Type Termx** that you custom defined.

Creating Terminal Definition Files

To create new terminal definition files, you need to copy and edit the information from the terminfo database.

1. On a UNIX host, change directory to `/usr/lib/terminfo/x` (where *x* is the first letter of the required terminal type). For a Wyse60, for example, you would enter the command `cd /usr/lib/terminfo/w`.
2. The termcap files are compiled, so use the command `infocmp termfile` to read the required file (for example: `infocmp wy60`).
3. Check the file for the attribute `xmc#n` (where *n* is greater than or equal to 1). This attribute will corrupt menu and form displays making the terminal type unsuitable for using Menu mode.
4. If the terminal definition is suitable, change to a directory of your choice.
5. Rename and copy the file to the directory specified at step 4. using the command `infocmp termfile > termn` where *n* is greater than or equal to 1; (for example, `infocmp wy50 > term1`). Make sure the file has global read and execute permission for its entire path.
6. Edit the file to include the following capabilities in this format:

```
term=
acsc=
bold=
civis=
clear=
cnorm=
cup=
rev=
rmacs=
rmso=
smacs=
smso=
page=
circ=
```


For example:

```
term=AT386 | at386| 386AT |386at |at/386 console
acsc=jYk?lZm@qDtCu4x3
bold=\E[1m
civis=
clear=\E[2J\E[H
cnorm=
cup=\E[%i%p1%02d;%p2%02dH
rev=\E4A
rmacs=\E[10m
rmso=\E[m
smacs=\E[12m
smso=\E[7m
page=
circ=n
```

Note: As you can see from the example, capabilities which are not defined in the terminfo file must still be included (albeit with no value). Each entry has an 80 character limit.

On some versions of UNIX, some of the capabilities are appended with a millisecond delay (of the form `$<n>`). These are ignored by the Terminal Server and can be left out.

The 'acsc' capability, if defined, contains a list of character pairs. These pairs map the characters used by the terminal for graphics characters to those of the standard (VT100) character set.

Include only the following character pairs:

jx, kx, lx, mx, qx, tx, ux and *xx*

(where *x* must be substituted by the character used by the terminal). These are the box-drawing characters used to display the forms and menus of Menu mode. They must be entered in this order.

The last two capabilities will not be found in the terminfo file. In the **page** field you must enter the escape sequence used by the terminal to change screens. The **circ** field defines whether the terminal can use **previous page** and **next page** control sequences. It must be set to **y** or **n**. These capabilities can be found in the documentation supplied with the terminal.

Resetting Configuration Parameters

You can reset the Terminal Server to its factory default settings (this will reset it to the original factory default or custom factory default settings, depending on what has been configured) through any of the following methods:

- You can push in the recessed button at the back of the Terminal Server hardware for three to ten seconds (pushing it in and then quickly releasing will just reboot the Terminal Server)
- DeviceManager, select **Tools**, **Reset**, **Reset to Factory Defaults**
- CLI, at the command line type, **reset factory**
- WebManager, select **Administration**, **Reset**, **Factory Default**, and then click the **Reset to Factory Defaults** button
- Menu, select **Network Configuration**, **Reset to Factory Defaults**
- SNMP, in the **adminInfo** folder, **set** the **adminFunction** variable to **2**

Lost Admin Password

If the Admin user password is lost, there are only two possible ways to recover it:

- reset the Terminal Server to the factory defaults
- have another user that has **admin** level rights, if one is already configured, reset the Admin password

A Virtual Modem AT Commands

Virtual Modem Initialization Commands

Note: Virtual Modem initialization commands are only supported on Terminal Server firmware and configurators version 3.2 or higher.

You can initialize the modem connection using any of the following commands:

Command	Description	Options
ATQn	Quite mode. Determines if result codes will be sent to the connected terminal. Basic results codes are OK, CONNECT, RING, NO CARRIER, and ERROR. Setting quite mode also suppresses the "RING" message for incoming calls.	n=0, result codes will be sent n=1 no result codes will be sent. (default)
ATVn	Verbose mode. Determines if result codes are displayed as text or numeric values.	n=0, display as numeric values. n=1, display as text. (default)
ATEn	Echo mode. Determines whether characters sent from the serial device will be echoed back by the Terminal Server when VModem is in "command" mode.	n=0, disable echo. n=1, enable echo. (default)
+++ATH	Hang up. This command instructs the Terminal Server to terminate the current session and go into "command" mode.	
ATA	Answer call. Instructs the VModem to accept connection requests. VModem will give the terminal up to 3 minutes to answer the call. If the ATA is not received within 3 minutes, all pending sync messages will be discarded.	
ATI0	Return the modem manufacturer name.	
ATI3	Return the modem model name.	
ATS0	Sets the value of the S0 register. The S0 register controls the "auto answer" behavior. In "manual" mode, the Terminal Server will not accept incoming sessions until an ATA is issued by the serial device. In "auto answer" mode, the Terminal Server will automatically accept an incoming connection request.	Register=0, sets "manual answer" mode Register=1-255, "auto answer" mode (default)

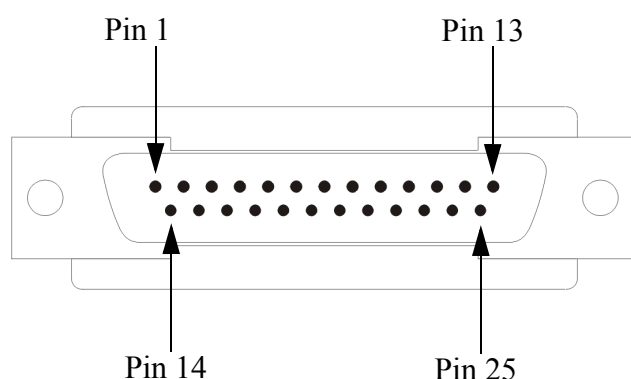
Command	Description	Options
AT&Z1	Set command allows the user to store an IP address and port number or phone number to use when making a connection. The user will issue an ATDS1 to cause the Terminal Server to initiate the connection.	
AT&Sn	Sets the behavior of Terminal Server's DTR signal. (DSR from a DCE perspective)	n=0, DTR signal always high. (default) n=2, DTR signal acts as DCD. n=3, DTR signal acts as RI.
AT&Rn	Sets the behavior of Terminal Server's RTS signal. (CTS from a DCE perspective) If line is configured for hardware flow control, the RTS is used for this purpose and the setting of this command is ignored.	n=0, RTS always high. (default). n=3, RTS signal acts as DCD. n=4, RTS signal acts as RI.
AT&Cn	Sets the behaviour of the DCD signal.	n=0, DCD always on. n=1, DCD follows state of connection (off when no connection, on when TCP connection exists). (default)
AT&F	Sets the modes back to the factory defaults. This is a hard-coded default configuration which does not look at any user configuration.	
ATS2	Sets the value of the S2 register. The S2 register controls which character is used to enter "command" mode. (this is the potential replacement for the +++ (default) in front of the ATH command). This register will hold the hex value of the "escape" character. Any value > 27 will disable the ability to escape into "command" mode.	
ATS12	Sets the value of the S12 register. The S12 register controls the minimum length of idle time which must elapse between the receipt of the escape character and the A (first character of the ATH sequence). Units are 1/50th of a second. The default is 50 = 1 second.	
ATO	(ATD with no phone number) Establishes a connection using the IP and port specified in the telephone number field.	
ATDS1	Establishes a connection using the IP and port (or phone number) specified in the Phone Number field (stored by the AT&Z1 command).	

B Pinouts and Cabling Diagrams

Serial Pinouts

DB25 Male

This section defines the pinouts for the DB25 male connection used on the 1-port Terminal Server.



The following table provides pinout information:

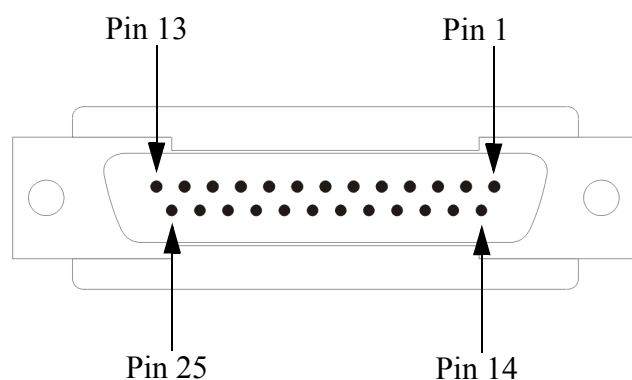
Pinout	EIA-232	EIA-422	EIA-485 Full Duplex	EIA-485 Half Duplex
1	Shield	Shield	Shield	Shield
2 (out)	TxD			
3 (in)	RxD			
4 (out)	RTS			
5 (in)	CTS			
6 (in)	DSR			
7	GND	GND	GND	GND
8 (in)	DCD			
12	Power in	Power in	Power in	Power in
13		CTS-		
14		TxD+	TxD+	DATA+
15		TxD-	TxD-	DATA-
18		RTS+		
19		RTS-		

Pinout	EIA-232	EIA-422	EIA-485 Full Duplex	EIA-485 Half Duplex
20 (out)	DTR			
21		RxD+	RxD+	
22		RxD-	RxD-	
25		CTS+		

The power in pin, pin 12, can be 9-30V DC.

DB25 Female

This section defines the pinouts for the DB25 female connection used on the 1-port Terminal Server.



The following table provides pinout information:

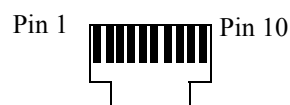
Pinout	EIA-232	EIA-422	EIA-485 Full Duplex	EIA-485 Half Duplex
1	Shield	Shield	Shield	Shield
2 (in)	RxD			
3 (out)	TxD			
4 (in)	CTS			
5 (out)	RTS			
6 (out)	DTR			
7	GND	GND	GND	GND
8 (in)	DCD			
12	Power in	Power in	Power in	Power in
13		RTS-		
14		RxD+	RxD+	
15		RxD-	RxD-	
18		CTS+		
19		CTS-		
20 (in)	DSR			

Pinout	EIA-232	EIA-422	EIA-485 Full Duplex	EIA-485 Half Duplex
21		TxD+	TxD+	DATA+
22		TxD-	TxD-	DATA-
25		RTS+		

The power in pin, pin 12, can be 9-30V DC.

RJ45

This section defines the pinouts for the RJ45 connection used on the Terminal Server.



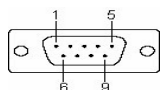
The following table provides pinout information:

Pinout 10-pin	Pinout 8-pin	EIA-232	EIA-422	EIA-485 Full Duplex	EIA-485 Half Duplex
1		Power In	Power In	Power In	Power In
2 (in)	1	DCD			
3 (out)	2	RTS	TxD+	TxD+	DATA+
4 (in)	3	DSR			
5 (out)	4	TxD	TxD-	TxD-	DATA-
6 (in)	5	RxD	RxD+	RxD+	
7	6	GND	GND	GND	GND
8 (in)	7	CTS	RxD-	RxD-	
9 (out)	8	DTR	RxD-	RxD-	

The power in pin, Pin 1, can be 9-30V DC.

DB9 Male

This section defines the pinouts for the DB9 male connection used on the 1-port Terminal Server.



The following table provides pinout information:

Pinout 9-pin	EIA-232	EIA-422/485 Full Duplex	EIA-485 Half Duplex
1 (in)	DCD		
2 (in)	RxD	RxD+	
3 (out)	TxD	TxD+	TxD+/RxD+
4 (out)	DTR		
5	GND	GND	GND
6 (in)	DSR	RxD-	
7	RTS		
8 (in)	CTS		
9		TxD-	TxD-/RxD-

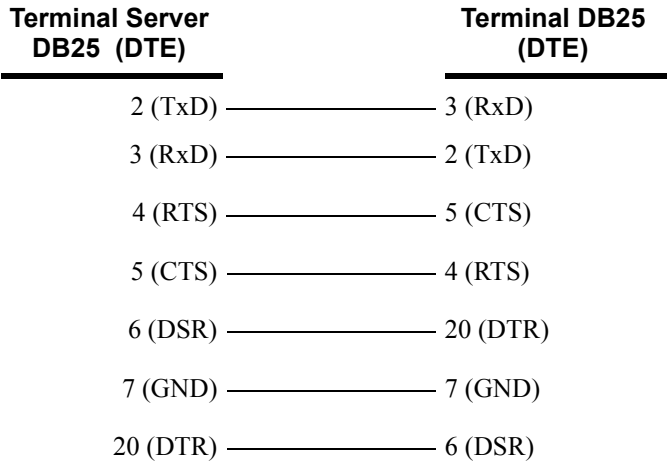
EIA-232 Cabling Diagrams

This section shows how to create EIA-232 cables that are compatible with the Terminal Server.

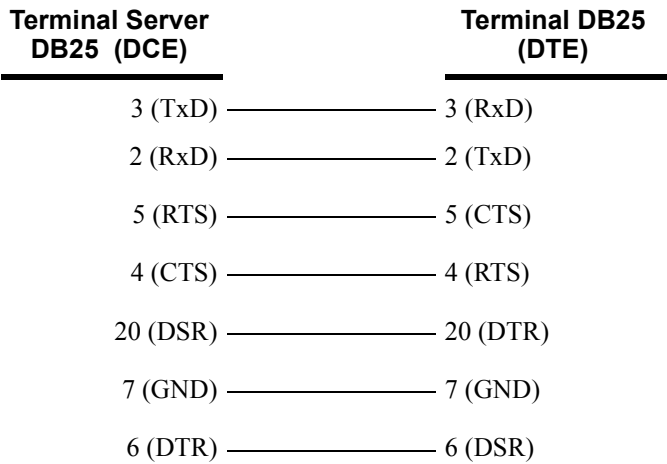
Terminal DB25 Connector

The following diagrams show how the null modem cable should be configured when connecting to a terminal DB25.

DB25 Male



DB25 Female



RJ45

Terminal Server RJ45		Terminal DB25 (DTE)	
10-pin	8-pin		
4 (DSR)	3	—————	20 (DTR)
3 (RTS)	2	—————	5 (CTS)
5 (TxD)	4	—————	3 (RxD)
6 (RxD)	5	—————	2 (TxD)
7 (GND)	6	—————	7 (GND)
8 (CTS)	7	—————	4 (RTS)
9 (DTR)	8	—————	6 (DSR)

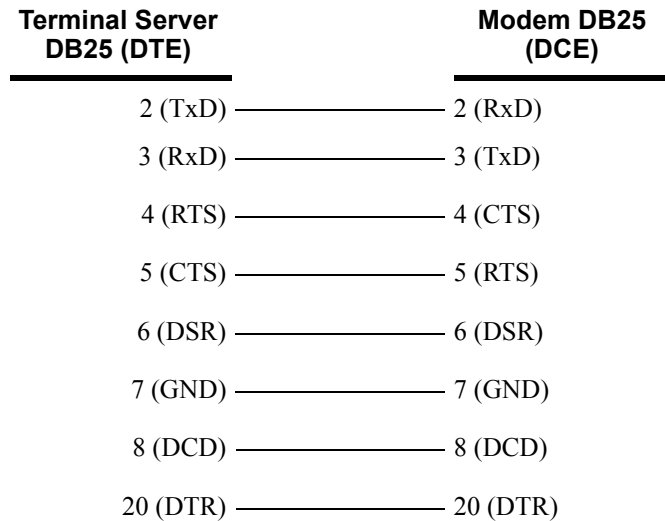
DB9 Male

Terminal Server DB9 Male	Terminal DB25 (DTE)
3 (TxD)	————— 3 (RxD)
2 (RxD)	————— 2 (TxD)
7 (RTS)	————— 5 (CTS)
8 (CTS)	————— 4 (RTS)
6 (DSR)	————— 20 (DTR)
5 (GND)	————— 7 (GND)
4 (DTR)	————— 6 (DSR)

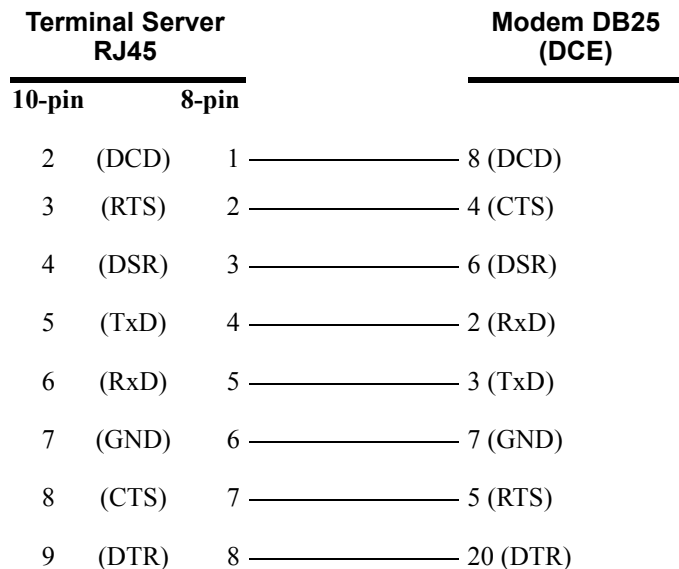
Modem DB25 Connector

The following diagrams show how a standard straight through cable should be configured when connecting to a DB25 modem.

DB25 Male



RJ45



DB9 Male**Terminal Server
DB9 Male****Modem DB25
(DCE)**

1 (DCD)	8 (DCD)
2 (RxD)	3 (TxD)
3 (TxD)	2 (RxD)
4 (DTR)	20 (DTR)
5 (GND)	7 (GND)
6 (DSR)	6 (DSR)
7 (RTS)	4 (CTS)
8 (CTS)	5 (RTS)

C Setting Jumpers

Introduction

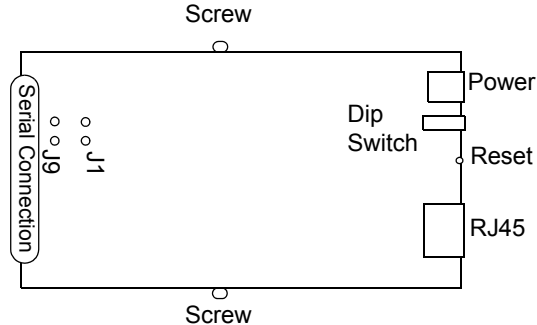
The Terminal Server contains jumpers that you might need to set before you configure it and put it into production. You can set the Terminal Server line termination to **on** or **off** (this is **off** by default) if you are using EIA-422/485.

1-Port Terminal Server

Terminal Server DB25 Male/Female

To change the settings, do the following:

1. Unplug the Terminal Server from the electrical outlet and disconnect everything from the box.
2. Open the case by unscrewing the two side screws, one on each side, and lifting off the top of the case. You should see the following:

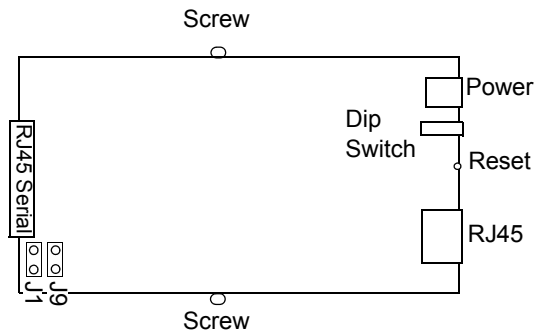


3. To turn line termination **on**, locate and jumper both J1 and J9.
4. Close the Terminal Server case by replacing the case lid and the two screws. You can now power it on with the new settings.

Terminal Server RJ45

To change the settings, do the following:

1. Unplug the Terminal Server from the electrical outlet and disconnect everything from the box.
2. Open the case by unscrewing the two side screws, one on each side, and lifting off the top of the case. You should see the following:

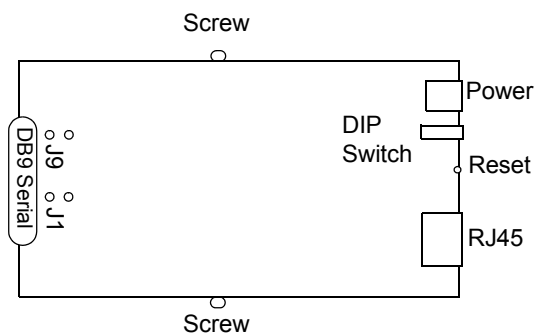


3. To turn line termination **on**, locate and jumper both J1 and J9.
4. Close the Terminal Server case by replacing the case lid and the two screws. You can now power it on with the new settings.

Terminal Server DB9

To change the settings, do the following:

1. Unplug the Terminal Server from the electrical outlet and disconnect everything from the box.
2. Open the case by unscrewing the two side screws, one on each side, and lifting off the top of the case. You should see the following:



3. To turn line termination **on**, locate and jumper both J1 and J9.
4. Close the Terminal Server case by replacing the case lid and the two screws. You can now power it on with the new settings.

D COMredirect Utility

Introduction

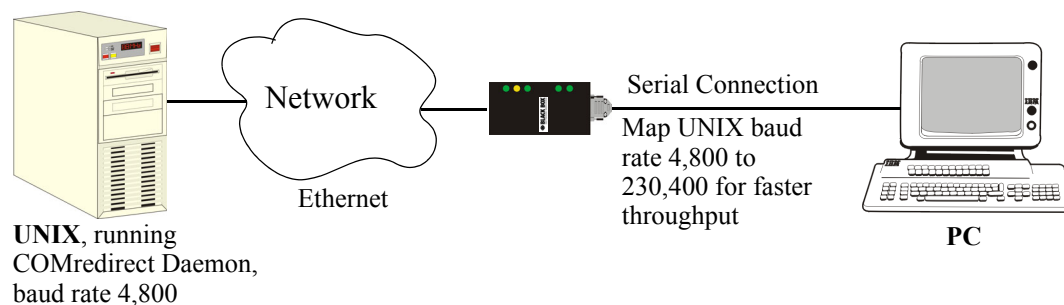
This chapter provides information on the COMredirect utility.

COMredirect

COMredirect is a com port redirector utility for the Terminal Server. It can be run in two modes:

- **COMredirect Full mode**—This mode allows complete device control and operates exactly like a directly connected serial port. It provides a complete COM port interface between the attached serial device and the network.
- **COMredirect Lite mode**—This mode provides a simple raw data interface between the device and the network. Although the port will still operate as a COM port, control signals are ignored. In this mode, the serial communications parameters must be configured on the Terminal Server.

You use COMredirect when you want to connect extra terminals to a server using a Terminal Server rather than a multi-port serial card. When run on UNIX, COMredirect allows you to print directly from a terminal to an attached printer (transparent printing). You can also remap the slow baud rate of your UNIX server to a faster baud rate, as shown below.



Currently, COMredirect is supported on Linux, Windows[®], SCO[®], Solaris[®], Unixware[®] and HP[®]. For more information, see the *COMredirect User Guide* for your platform or the *COMredirect Installation and Configuration Guide for Windows NT[®]* on the CD-ROM.

E

Troubleshooting

Introduction

This chapter provides information that can help resolve problems with the Terminal Server.

Hardware Problems

If the Terminal Server Power/Ready LED is red and stays red for over 10 seconds, you have a hardware problem that might require factory service. First, try the following:

- If the Terminal Server is not in Console mode, do the following:
 - a. Set up a direct connection to the Terminal Server; see [Through the Serial Port](#) for information on this type of connection.
 - b. Power the Terminal Server off.
 - c. Switch the Console dip switch to On.
 - d. Power the Terminal Server on.

If there is a problem with the Terminal Server firmware, you will need to reload the firmware, which can be found either on the CD-ROM that came with the Terminal Server.

- If the Terminal Server is already in Console mode and the Power LED stays red, you need to make arrangements to return the Terminal Server.

If you purchased the Terminal Server less than 30 days before this problem appears, contact your distributor; otherwise, see the Black Box web site (www.blackbox.com) for factory service information. Note: no factory service can be done on a Terminal Server that has not been registered.

Power/Ready LED continues to flash green in Desktop models

This is not an error, the Power/Ready LED will flash green when serial port 1 is in Console Mode.

Communication Issues

General communication checks and practices are as follows:

- Are your cables connected and correctly configured? If you are using EIA-232, see [EIA-232 Cabling Diagrams](#) to verify that your cables are correctly configured.
- Ping your host? If you can ping but packet loss is reported, ping another host/device on the same network. This will tell you whether the problem is specific to the host/device or general to the network.
- After entering or changing IP information for your Terminal Server, *reboot* the Terminal Server (does not apply when using BOOTP or DHCP). Once the Terminal Server has rebooted, other network devices should be able to communicate with it (ping, telnet, etc.). Also, protocols such as ARP and proxy-ARP will work properly.
- Use the **show routes** command (command line only) or view the **Routes** statistics. Is there a route to the host?

- If the WebManager or DeviceManager cannot communicate with the Terminal Server, verify that the **Security, Services HTTP** parameter is enabled for WebManager and **DeviceManagerD** is enabled for DeviceManager.

DeviceManager Problems

Error Message: **16 bit Windows Subsystem - C:\WINDOWS\SYSTEM32\AUTOEXEC.NT. The system file is not suitable for running MS-DOS and Microsoft Windows applications. Choose 'Close' to terminate the application.**

The error message can be misleading, because it is displayed even if the **AUTOEXEC.NT** file is actually missing.

To verify whether you have the file, type `%windir%/system32/` in the address bar of an Explorer window. If there is no **AUTOEXEC.NT** file proceed as follows:

1. Browse to `%windir%/repair/` (usually `C:\WINDOWS\repair`).
2. Right-click and Copy the **AUTOEXEC.NT** file.
3. Browse to `%windir%/system32/` (usually `C:\WINDOWS\System32`).
4. Right-click inside the window and Paste the file.

The error condition described here may also be the result of corruption of the **AUTOEXEC.NT** file, in which case the above procedure may be helpful to restore a valid file.

If the above procedure does not fix the DeviceManager installation problem, see <http://support.microsoft.com/?kbid=324767> for the official Microsoft explanation.

Host Problems

Cannot access a host on a local network, verify:

- The network address is correct.
- The subnet mask is set correctly and reflects the network configuration.
- The broadcast address is set correctly and reflects the network configuration.

Cannot access a host on a remote network:

- Use the **show route** command to verify that there is a route to the remote host. If no gateway is specified, verify that a default gateway is specified. Ping the default gateway to check if it is working.
- Consider the situation beyond the gateway; for example, are intermediate gateways and the remote host available? Also, check the messages returned by the **ping** command; for example, that a particular host or gateway is unreachable.

Gateways added into the gateway table are ignored by the Terminal Server:

- Have you used BOOTP and entered a single static gateway in the bootptab file entry? If yes, the other gateways will be ignored.

Access to host lost after a few minutes.

- If the route to this host goes through routers, make sure those routers are all sending RIP packets across the networks.

Login Problems

You have lost or don't know your password (as Admin user).

- You must reset the Terminal Server to its factory default settings using the **Reset** switch on the rear panel. There is no procedure to access the Terminal Server without a password.

Problems with Terminals

The following section concerns problems with the appearance of data on your terminal screen.

The Terminal Server logs me out after a few minutes:

- Check the **Idle Timer** value set for the user. The default setting for the **Idle Timer** for all users is 0 seconds (does not timeout).

Corrupt data.

- Check your line settings (baud rate, stop bits, etc.)

Missing data.

- Verify that the same type of flow control is set in both your terminal and on the Terminal Server's port.

Error message not permitted on a dumb terminal after typing the CLI command screen.

- Set your **Line** to **Termtypes** VT100, ANSI or WYSE60 (or other form of terminal emulation, if you have downloaded one). The default line type in the Terminal Server is **Dumb**, which does not support the graphics characters necessary to view the text-based menus.

Screen corruption when using the text-based menu system.

- Verify that the terminal setup in the Terminal Server matches your terminal.
- Verify that entries in the term file match your terminal setup.
- If using a PC/computer, verify that the type of terminal emulation selected in your application matches those supported by the Terminal Server.

When using the function keys on your keyboard, nothing happens or your sessions keep swapping.

- Change your **Hotkey Prefix** character. The function keys on the keyboards of some terminals (like WYSE60) send character sequences which begin with **^a**; unfortunately, **^a** is also the default **Hotkey Prefix**, which you use to switch between sessions. A valid alternative would be **^b** (hex=02). If you are the system administrator, you can change any user's **Hotkey Prefix** character.

When using a downloaded terminal definition, you are having problems using arrow keys.

- Use Ctrl-K, Ctrl-J, Ctrl-H and Ctrl-L for up, down, left and right respectively.

When switching from a session back to the text menus, both screen images are superimposed.

- Press **^r** to redraw the screen.

INIT: Error in terminal file <filename>

- This error indicates that you have exceeded the 80 character limit for one or more of the terminal capabilities defined in the reported file.

INIT: Error on line n in terminal file <filename>

- You have omitted the = sign from the reported line.

Unknown IP Address

You have a Terminal Server already configured and you do know your password, but have lost, misconfigured, or don't know the IP address of the Terminal Server, and you cannot obtain a login.

- If the Terminal Server resides within the local network segment, you can use DeviceManager to find the Terminal Server.
- You can connect directly to the serial port of the Terminal Server, as explained in [Through the Serial Port](#).

DHCP/BOOTP Problems

Messages: host name too long or filename too long.

- The Terminal Server can only accept host names of 14 characters or file names of 64 characters, so verify that you are not attempting to pass a string that is longer than those maximums.

DHCP or BOOTP have been set up to configure my Terminal Server, but does not seem to have done anything.

- Check that the server DHCP/BOOTP service is set to on, if not set it to on and reboot.
- Check that your BOOTP server is configured for your Terminal Server or that your DHCP server has an active lease pool (scope) with at least 1 free IP address.

You observe TFTP errors when the Terminal Server boots, for example:

TFTP: File not found : filename

TFTP: Timed out

This has a number of causes, including:

- The file names you specified to DHCP/BOOTP do not exist or are in the wrong place.
- The server for any of the downloadable files in your bootfile has no TFTP server running.
- Verify that lease data in your DHCP server manager is correct.
- Reset or restart the DHCP server.

Language Problems

In a customized language, the text strings appear in the wrong place in the Menu, CLI, or WebManager.

- Check the original ASCII text file you used to translate to your customised language. The sequence of the line much match exactly (be aware that comments don't affect line sequence, but can affect the actual line that the strings appear on). So, if you strip out all comments, if the original file says line 1000 should be string **none**, then line 1000 (stripped of comments) should be the translated version of **none**.

Long Reboot Cycle

Rebooting the Terminal Server takes a long time.

If you are not using DHCP/BOOTP, disable this within the Server Services; otherwise, the Terminal Server waits to timeout for a request to DHCP/BOOTP.

IPv6 Issues

You are not seeing the IPv6 address value when you attempt to connect to the Terminal Server.

Many Windows® based systems have IPv6 support already enabled, however, if you need to install IPv6 then follow the procedure below.

To install IPv6 support in Windows® do the following:

1. In Control Panel, double-click the **Network Connections** icon.
2. Double-click the **Local Area Connection** entry.
3. In the Local Area Connection Status window, click the **Properties** button on the **General** tab.
4. In the Local Area Connections window, click the **Install** button on the **General** tab.
5. In the Select Network Component Type window, select **Protocol** and click the **Add** button.
6. In the Select Network Protocol window, select **Microsoft TCP/IP version 6** and click the **OK** button.

G Data Logging

Introduction

This appendix provides additional information about the Data Logging feature.

COMredirect Profile

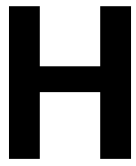
The following features are not compatible when using the Data Logging feature.

- Allow Multiple Hosts to connect
- Connect to Multiple Hosts
- Monitor DSR or DCD
- Signals high when not under COMredirect client control
- Message of the day
- Session timeout

TCP Socket Profile

The following features are not compatible when using the Data Logging feature.

- Allow Multiple Hosts to connect
- Connect to Multiple Hosts
- Monitor DSR or DCD
- Permit connections in both directions
- Authenticate user
- Message of the day
- Session timeout



Modbus ReMapping

Introduction

This appendix provides additional information about the Modbus Remapping feature.

Modbus Remapping Feature

The Modbus remapping feature allows a TCP Modbus Master to poll a Modbus slave device and have the Terminal Server translate the UID to a different UID for the slave device. The Master UID has to be unique on the Terminal Server. The Slave UID must be unique on each serial port. The translate rules are controlled by a file downloaded to the Terminal Server.

The following procedure will allow you to use the Modbus remapping feature:

Create a configuration file

- The file must be called "modbus_remap"
- One translate rule per line
- The fields on a line are separated by a comma

Line format for one UID is:

port,master_uid,slave_uid

- port: is the Terminal Server port number that the slave is connected to
- master_uid: is the UID that the TCP Modbus Master uses
- slave_uid: is the UID that the Modbus slave uses

Line format for UID ranges is:

port,master_start-master_end,slave_start-slave_end

- port: is the Terminal Server port number that the slave is connected to
- master_start: is the first master UID in the range
- master_end: is the last master UID in the range
- slave_start: is the first slave UID in the range
- slave_end: is the last slave UID in the range

Configuring the Modbus UID Translation Feature

1. On the serial port Modbus Gateway, configure Modbus slave. Configuration parameters such as “UID range” and UID Address Mode will be ignored in this mode of operation
2. Down load the "modbus_remap" file that you created to the Terminal Server using:
 - Device Manager: use "tools-advanced-custom files" dialog "download other file"
 - Web Manager: use "administration-custom files" page "other file"
 - CLI: use the command "netload customapp-file" command

Index

A

admin

- default password [40](#)
- lost password [146](#)

ARP-Ping, setting an IP address [42](#)

B

binary configuration file [53](#)

BOOTP

- parameters [35](#)
- setting an IP address [41](#)

C

cabling, EIA-232 [153](#)

COMredirect utility [67](#), [159](#)

configuration files

- formats [53](#)

connecting to the Terminal Server

- console mode [22](#)
- serial mode [22](#)
- setting IP address [24](#)

console mode [22](#)

custom factory default configuration [140](#)

D

DB25

- pinouts
 - female [150](#)
 - male [149](#)
- power in pin
 - female [151](#)
 - male [150](#)

DB9 male pinouts [152](#)

default admin password [40](#)

definitions [164](#)

DeviceManager

- overview [27](#)
- setting an IP address [39](#)

DHCP

- parameters [35](#)
- setting an IP address [41](#)

direct connect

- setting an IP address [40](#)

F

factory default configuration

- custom [140](#)
- original [140](#)

factory defaults, resetting to [145](#)

I

IPv6, setting an IP address [42](#)

J

jumpers

- line termination [157](#)
- setting [157](#)

L

language

- translating [143](#)
- upgrading firmware [143](#)

line termination, setting jumper [157](#)

M

Menu

- conventions [33](#)

MIB [35](#)

mode

- console [22](#)
- serial [22](#)

modem parameters [109](#)

O

online help, using [16](#)

P

parameters

BOOTP/DHCP [35](#)

modems [109](#)

password

admin default [40](#)

lost [146](#)

pin, power in

DB25 female [151](#)

DB25 male [150](#)

serial RJ45 [151](#)

pinouts

DB25 female [150](#)

DB25 male [149](#)

DB9 male [152](#)

RJ45 serial [151](#)

power in pin

DB25 female [151](#)

DB25 male [150](#)

serial RJ45 [151](#)

R

resetting to factory defaults [145](#)

RJ45

serial pinouts [151](#)

RJ45 serial power in pin [151](#)

S

serial mode [22](#)

services

line

UDP [81](#)

vmodem [95](#)

sessions [126](#)

setting an IP address

ARP-Ping [42](#)

BOOTP/DHCP [41](#)

DeviceManager [39](#)

direct connect [40](#)

IPv6 [42](#)

SNMP

support MIBs [36](#)

using [35](#)

T

terminal definitions

creating [144](#)

downloading [144](#)

text configuration file [53](#)

U

UDP

configuring [81](#)

user sessions [126](#)

utility

COMredirect [67](#), [159](#)

V

virtual modem [95](#)

vmodem

overview [95](#)

W

WebManager

overview [30](#)

Glossary

This chapter provides definitions for Terminal Server terms.

BOOTP (BOOTstrap Protocol)	An Internet protocol that enables a diskless workstation to discover its own IP address, the IP address of a BOOTP server on the network, and a file to be loaded into memory to boot the machine. This enables the workstation to boot without requiring a hard or floppy disk drive.
Callback	A security feature where the Terminal Server calls back the User at a predetermined number defined in the User's account.
Community (SNMP)	An SNMP community is the group that devices and management stations running SNMP belong to. It helps define where information is sent.
DHCP (Dynamic Host Configuration Protocol)	A TCP/IP protocol that provides static and dynamic address allocation and management.
Direct Connection	Connections that bypass the Terminal Server enabling the user to log straight into a specific host. A direct connection is recommended where a user logging in to the Terminal Server is not required.
Ethernet	A high-speed (10Mbps,100Mbps) cable technology that connects devices to a LAN, using one or more sets of communication protocols.
Fixed Callback	A method where there is a specific number defined to callback a user.
Local Authentication	Uses the user ID and password stored within the Terminal Server User database.
LPD	Line Printer Daemon. A printer protocol that uses TCP/IP to establish connections between printers and workstations on a network. The technology was developed originally for BSD UNIX and has since become the de facto cross-platform printing protocol.
Modem Initialization String	A series of commands sent to the modem by a communications program at start up. These commands tell a modem how to set itself up in order to communicate easily with another modem.
MOTD	Message of the day. This is defined by a file whose contents display when users log into the Terminal Server.
Multicast	The broadcasting of messages to a specified group of workstations on a LAN, WAN, or internet.
NAK (Negative Acknowledgment)	A communication control character sent by the receiving destination indicating that the last message was not received correctly.
RADIUS (Remote Authentication Dial In Users Services)	An open standard network security server that communicates with the PAP protocol.
Reverse Connection	Connections that originate from a host that go directly to a serial device through the Terminal Server.

RIP (Routing Information Protocol)	A protocol that allows gateways and hosts to exchange information about various routes to different networks.
Roaming Callback	A method where the client supplies the number for callback when they dial in.
RPC	Remote Procedure Call. A type of protocol that allows a program on one computer to execute a program on a server computer.
Silent Connection	Silent connections are the same as direct connections except that they are permanently established. The host login prompt is displayed on the screen. Logging out redisplay this prompt. Silent connections, unlike direct connections, however, make permanent use of pseudo tty resources and therefore consume host resources even when not in use.
SNMP (Simple Network Management Protocol)	A protocol for managing network devices.
Subnet/Prefix Bits	Identifies the device's IP address, which portion constitutes the network address and which portion constitutes the host address.



© Copyright 2016. Black Box Corporation. All rights reserved.

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