SIXNET® User Manual

EtherTRAK® Industrial Ethernet Device Server

DS1 User’s Guide

Version 2.0

Part# ET-DS-2

November 2006

SIXNET
331 Ushers Road
PO Box 767
Clifton Park, NY 12065

SIXNET reserves the right to make changes without further notice, to any products to improve reliability, function, or design.

FCC Note The SIXNET Device Server has been found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions in this Guide, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his/her own expense.

EN 55022: 1998, Class A, Note

WARNING This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

CE **Caution:** The SIXNET Device Server is approved for commercial use only.

Table of Contents

Preface

About This Book

This guide provides the information you need to:

- configure the Device Server
- incorporate the Device Server into your production environment

Intended Audience

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

Documentation

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

- *SIXNET DS1/SDS1 Device Server Quick Start Guide*
- *SIXNET Device Server User's Guide*
- *COMredirect 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: `add host`	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.

`subscribe` *`project`* *`subject`*
`run` ***`yourcode`*** **`.exec`**
	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 *`project`*, you enter your own value, such as `stock_trader`, and for ***`yourcode`***, 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.
SIXNET User's Guide	This typeface indicates a book or document title.
See ***Chapter 1, Introduction on page 15*** 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's Guide* online by selecting **Help**, **Help Topics**.

1 Introduction

About the SIXNET Device Server

The Device Server is an ethernet communications/terminal server that allows serial devices to be connected directly to LANs. The Device 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.)
- PCs using terminal emulation
- Modems for remote access and Internet access
- ISDN adapters for branch remote access and Internet access
- All types of serial printers

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

SIXNET Device Server Models

The SIXNET Device Server comes in several different models to meet your production environment needs:

- **DS**—Offered as an RJ45 1-port unit, this model provides basic Device Server functionality.
- **SDS**—This model does everything the DS model does plus additional features such as external authentication, SSH, SSL, port buffering, email alerts, RIP, DNS/WINS, plus much more. This model has an EIA-232/422/485 switchable interface.

Device Server Features

The Device Server is a communications server with 1 port for making serial network connections. It attaches to your TCP/IP network and allows serial devices such as modems, terminals, or printers to access the LAN.

Hardware

The Device Server hardware features include:

- Auto sensing 10/100 RJ45 interface.
- Universal, software-selectable EIA-232/422/485 interface.
- Full modem control using DTR, DSR, CTS, RTS and DCD.
- Tx and Rx activity indicators.
- External AC power supply or power over serial.
- LEDs for diagnostic testing.
- Self-test on power-up.
- Reset switch.

Software

The Device Server software features include:

- Multiple ways to configure the Device Server:
  - Easy Config Wizard, an easy configuration wizard that allows you to complete basic Device Server configuration
  - DeviceManager, a fully functional Windows 98/NT/2000/ME/Server 2003/XP configuration/management tool
  - WebManager, a web browser option for configuring/managing the Device 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 Device Server
- IPv6 support.
- Support for TCP/IP and UDP protocols telnet.
- Virtual modem emulation.
- ‘Fixed tty’ support for several operating systems (COMredirect).
- DHCP/BOOTP for automated network-based setup.
- Dynamic statistics displays and line status reporting for fast problem diagnosis.
- Multi session support on a single terminal.
- Interoperability with IP routing through gateway tables.

Security

The Device Server security features include:

- Supervisory and port (line) password.
- Port locking.
- Per user access level assignment.
- Logging via Syslog.
- Idle port timers, which close a connection that has not been active for a specified period of time.
- Ability to individually disable daemons/services that won't be used by the Device Server.

Supported Products/Versions

Web Browsers

The WebManager has been tested on Windows and Linux with the following web browsers:

- **Netscape**—7.x
- **Internet Explorer**—6.x
- **Mozilla Firefox**—1.x

Typical Applications Summary

Managing the Device Server

The Device Server can be managed and configured by administrators through various methods, allowing them full configuration capabilities and easy access to management statistics and tools. Administrators can access the Device Server using the following methods:

- Connection through ethernet using the DeviceManager, a Windows-based configuration application.
- Connection through ethernet using WebManager, via a web browser.
- Direct connection to the serial port using a Serial Terminal or Terminal Emulation Software.
- From the network through the ethernet interface using reverse Telnet (Port 23).
- Through an SNMP agent, using the Device Server MIB.

Managing/Accessing devices attached to the Device Server

The Device Server can be configured to allow users or administrators to view or manage specific devices on the Device Server's serial port across the Ethernet interface using two different methods.

- **Direct Connect**—users can directly connect to the device on the serial port by Telnet (**Line Service** must be set to **Rev Telnet**) using the Device Server's configured IP address and the serial device's assigned TCP port number.
- **Easy Port Access**—users can connect to the Device Server using the configured Device Server's IP address by reverse Telnet (port number 23), and are provided with a device menu displaying the name of the device that the user has access to. This feature eliminates the need for administrators and users to recall the specific port number associated with a certain device connected to the Device Server. The user can simply connect to a specific device based upon the name of the device and then return to the device menu without disconnecting its initial reverse Telnet connection.

Network Security

The Device Server provides a comprehensive suite of security features to allow an organization to implement robust security planning to prevent unauthorized access. These include trusted host filtering and the ability to disable individual services.

2 Installation

Introduction

This chapter tells you what is packaged with your SIXNET Device Server, how to power up the Device Server to make sure it works correctly, and how to assign the Device Server an IP address through the LAN.

SIXNET Device Server Components

What's Included

When you open your SIXNET Device Server package, you should have the following components:

- The Device Server
- A CD-ROM containing documentation, firmware, DeviceManager, etc.

What You Need to Supply

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

- A serial cable
- An ethernet 10/100BASE-T cable if you are connecting the Device Server to the network
- Power supply

Available Accessories

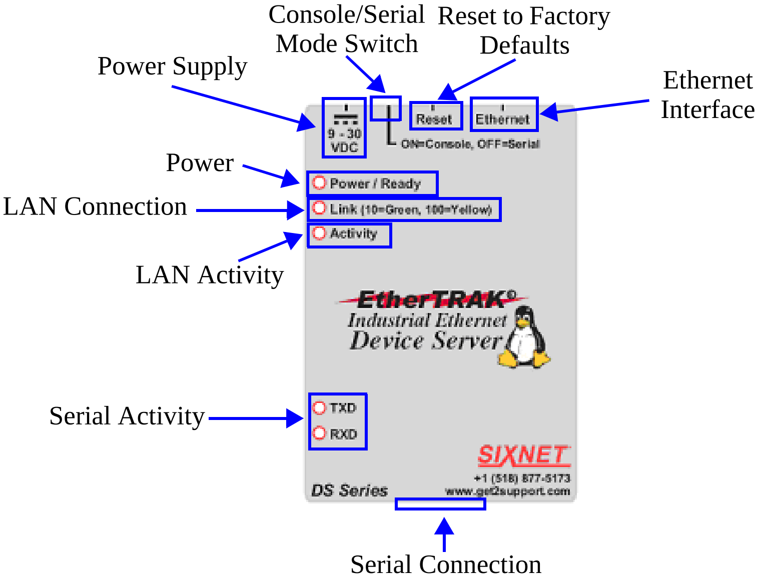
The following accessory is available for purchase for the Device Server:

- DIN Rail Mounting Kit (35mm)

Contact your distributor for details.

Getting to Know Your Device Server

This section describes the components found on the Device Server.



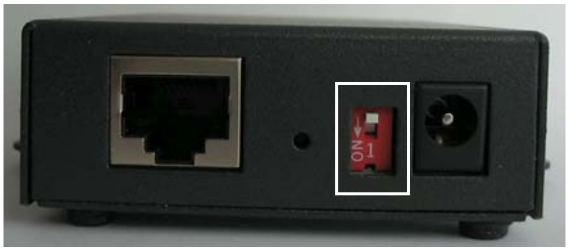
LED Guide

The Device Server LEDs display the following information:

- **Power/Ready**—(Green/Red/Yellow) Shows red at power up. If this LED remains red, indicates that there is a critical error (return to factory). Flashes green to indicate that the Device Server is booting. Flashes green/yellow when the firmware is being updated. Stays solid green to indicate that the Device Server is ready.
- **Link/10/100**
  - Green—10 Mbits
  - Yellow—100 Mbits
  - Off—no LAN connection
- **Activity**—Flashes Green for transmit (TX) or receive (RX) LAN data
- **Tx**—Flashes with transmit serial activity
- **Rx**—Flashes with receive serial activity

Console Mode vs. Serial Mode

You will notice a little switch at the back of the Device Server for switching the Device Server to either Console or Serial mode.



When the switch is down (ON), the Device Server is in Console mode; when the switch is up, the Device Server is in Serial mode. Console mode is used when you have a direct connection between a serial device (like a terminal or a PC) and the Device Server, accessed by the Admin user to configure/manage the Device Server. You can connect directly to the Device Server in Serial mode, but the Device Server will not display all the messages/information you will get in Console mode. Console mode automatically sets the **Serial Interface** to **EIA-232**, **Speed** to **9600**, **Flow Control** to **No**, **Bits** to **8**, **Stop Bits** to **1**, and **Parity** to **None**, in addition to displaying extra system messages. Your Device Server will not work in a production environment in Console mode.

Serial mode is used when the Device Server acts as a communications server, or anytime you are not connecting directly to the Device Server to configure it.

Powering Up the Device Server

Before you attach the Device Server to your network or try to configure it, we suggest that you power it up to verify that it works properly. To power up the Device Server, perform the following steps:

1. Plug the external power supply into the Device Server and then into the electrical outlet.
2. If the Device Server is working correctly, you should see:
   a. The Power/Ready LED starts out red.
   b. The Power/Ready LED flashes green while the Device Server boots up.
   c. The Power/Ready LED stays solid green, indicating that it is ready to configure/use.

You are now ready to begin communicating with your SIXNET Device Server. The last step of the installation process is to set an IP address for the Device Server; this is necessary before it can be configured and put into production.

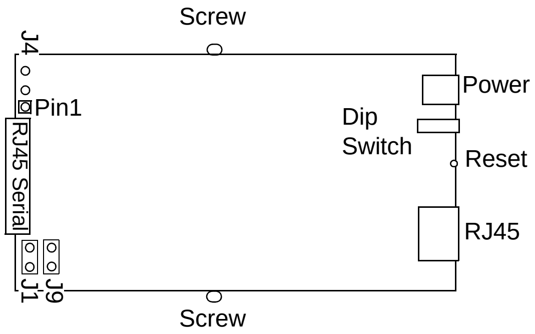
Before you start to configure the Device Server, you should set the Device Server jumpers if you want to terminate the line.

Setting Jumpers

The Device Server contains jumpers that you might want to set before you configure it and put it into production. You can set the power out pin to a fixed 5V DC output or to the external adapter output; this can range from 9-30V DC (the external adapter that is shipped with the Device Server has a 12V DC output). By default, the power out pin is set to no power. You can set the Device Server line termination to **on** or **off** (this is **off** by default) if you are using EIA-422/485.

To change the settings, do the following:

1. Unplug the Device 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 change the power pin out, locate J4. For the fixed 5V DC output, jumper pins 1 and 2. For the output to equal the external adapter input, jumper pins 2 and 3.
4. To turn line termination **on**, locate and jumper both J1 and J9.
5. Close the Device Server case by replacing the case lid and the two screws. You can now power it on with the new settings.

Setting an Initial IP Address

This section describes the different methods you can use to set the Device Server IP address.

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

- **Easy Config Wizard**—The Easy Config Wizard is automatically launched from the CD ROM included with your **Device Server**. You can use the Easy Config Wizard to set the **Device Server**'s IP address and configure the line(s).
- **DeviceManager**—Use this method when you can connect the Device Server to the network and access the Device Server from a Windows® PC. The DeviceManager is a Windows-based application that can be used for Device Server configuration and management.
- **Direct Connection**—Use this method when you can connect the Device Server directly to a dumb terminal, essentially logging directly into the Device Server. Using this method, you will need to configure and/or manage the Device 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 Device Server to your network. The Device Server will automatically obtain an IP address from a local network DHCP/BOOTP server when this service is enabled (it is disabled by default).
- **ARP-Ping**—Use this method when you can connect the Device Server to the network and want to assign a temporary IP address to the Device Server by specifying an ARP entry and then pinging it.

- **IPv6 Network**—When the Device Server is connected to an IPv6 network, its local link address should automatically be recognized by the network.

Note: Regardless of which method you use, the Device Server must reside within the same network as the host you are accessing it from.

Once an IP address has been assigned to the Device Server, in most cases, you can continue to use the same method to configure and/or manage the Device Server. See Chapter 3, ***Configuration Methods*** on page 29 for more information on the different methods you can use to manage/configure the Device Server.

Using DeviceManager

To use the DeviceManager, you must first install it on a Windows 98/2000/NT/ME/Server 2003/XP operating system (Windows NT requires Service Pack 4 or later) that resides in the same network as the Device Server. The DeviceManager installation wizard can be found on the CD-ROM included in the Device Server package.

1. Connect the Device Server to the LAN and plug it in; it will automatically boot up.
2. From the CD-ROM that was included in the Device Server packaging, select the DeviceManager link.
3. Click on the link under **Location** and click **Open** to automatically start the DeviceManager installation.
4. 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.
5. On the **Manage Device Server** tab, click the **Search Local Network** button.
6. Any Device Server that does not have an IP address will be displayed as **Not Configured**, with the **Model** and **MAC Address** to identify the Device Server. Highlight the Device Server that you want to assign an IP address to and click the **Assign IP** button.

   Note: If your Device Server is displayed with an IP address at this point, you are running a DHCP/BOOTP server on your network and the Device Server has obtained an IP address already. If you want to permanently assign an IP address, continue following the directions, if the DHCP/BOOTP assigned IP address is sufficient, you are now ready to configure the Device Server.

7. Type in the IP address that you want to assign to this Device Server and click the **Assign IP** button.

   Note: This is just a temporary IP address that you can use to open a session to the Device Server for configuration.

8. You are now ready to configure the Device Server. Double-click the Device Server you just assigned the temporary IP address to, to open a configuration session. Type **`superuser`** (the factory default Admin user password) in the Login window and click **OK**.
9. Expand the **Server Configuration** folder and select **Server**. You can choose to enter a permanent IP address in the **Internet Address** field and the **Subnet/Prefix Bits** field of the Server window.

   Note: If your network runs a DHCP server and you don't want the Device Server to obtain its **IP Address** from the DHCP server (or if you're not sure if there is a DHCP server and you want to assign a permanent **IP Address**), disable the **DHCP/BOOTP Service** in this window.

10. Click the **Apply** button when you're done with the Server window. To permanently assign the IP address, you need to download the new configuration file and then reboot the Device Server.
11. Download the configuration file to the Device Server by selecting **Tools**, **Download Configuration to Unit**.

12. Reboot the Device Server by selecting **Tools**, **Reboot Server**.

For more information on configuring the Device Server using DeviceManager, see Chapter 5, ***Using the DeviceManager*** on page 51.

Using a Direct Connection

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

1. Connect the Device Server to your PC or dumb terminal. Make sure the dip switch is in Console mode (this sets the Device 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). See ***EIA-232 Cabling Diagrams*** on page 27 for cabling diagrams.
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 Device Server.
3. When prompted, type **`admin`** for the User and **`superuser`** for the Password. You should now see the **`DS1#`** prompt.
4. You are now logged into the Device Server and can set the IP address by typing from the command line using the Command Line Interface (CLI):

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

   Where ***`ipv4address`*** is the IP Address being assigned to the Device Server.
5. Type the following command:

   ```
   save
   ```
6. If you are going to use another configuration method, such as WebManager or DeviceManager, unplug the Device Server. Change the Device Server dip switch to Off Serial (dip switch in the up position) and connect it to your serial device. Plug the Device Server back in, automatically rebooting the Device Server in the process.
7. If you want to complete the configuration using a direct connection, see Chapter 3, ***Configuration Methods*** on page 29 and/or Chapter 6, ***Command Line Interface*** on page 87. After you complete configuring the Device Server, unplug the Device Server. Change the Device Server dip switch to Off Serial (dip switch in the up position) and connect it to your serial device. Plug the Device Server back in, automatically rebooting the Device Server in the process.

Using DHCP/BOOTP

If you are using BOOTP, you need to add an entry for the Device Server that associates the MAC address (found on the back of the Device Server) and the IP address that you want to assign to the Device 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 Device Server using a PC with a terminal emulation package, such as HyperTerminal or a terminal.

1. Connect the Device Server to your PC or dumb terminal. Make sure the DIP switch is in Console mode. When connecting a terminal or PC directly (without modems), the EIA-232 signals need to be crossed over ('null modem' cable). See ***EIA-232 Cabling Diagrams*** on page 27 for cabling diagrams.
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 Device 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, **`DS1#`**.

4. You are now logged into the Device 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 service dhcp/bootp on
   ```
5. Type the following command:

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

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

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

You are now ready to configure the Device Server. See Chapter 3, ***Configuration Methods*** on page 29 for information on the different Device 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 Device 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:

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

   On a Windows® 98 or newer system, type the following:

   ```
   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 Device Server, and **aa:bb:cc:dd:ee:ff** is the Ethernet (MAC) address of Device Server, found on the back of the unit.
2. Whether you use UNIX or Windows®, you are now ready to ping to the Device 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
   ```

You are now ready to configure the Device Server. See Chapter 3, ***Configuration Methods*** on page 29 for information on the different Device Server configuration methods.

IPv6 Network

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

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

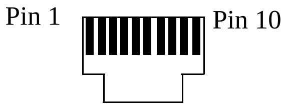
Link Local Address: fe80::0280:D4ff:feAB:CDEF

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

You are now ready to configure the Device Server. See Chapter 3, ***Configuration Methods*** on page 29 for information on the different Device Server configuration methods.

Pinouts

This section defines the pinouts for the RJ45 connection used on the Device 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	TxD+/RxD+
4 (in)	3	DSR			
5 (out)	4	TxD	TxD-	TxD-	TxD-/RxD-
6 (in)	5	RxD	RxD+	RxD+	
7	6	GND	GND	GND	GND
8 (in)	7	CTS	RxD-	RxD-	

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

EIA-232 Cabling Diagrams

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

Terminal DB25 Connector

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

SIXNET 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)

Modem DB25 Connector

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

SIXNET RJ45			Modem DB25 (DCE)
10-pin		**8-pin**	
2	(DCD)	1	8 (DCD)
3	(RTS)	2	4 (CTS)
4	(DSR)	3	6 (DSR)
5	(TxD)	4	2 (RxD)
6	(RxD)	5	3 (TxD)
7	(GND)	6	7 (GND)
8	(CTS)	7	5 (RTS)
9	(DTR)	8	20 (DTR)

3 Configuration Methods

Introduction

This chapter provides information about the different methods you can use to configure the Device Server.

DeviceManager

The DeviceManager is a fully functional Windows 98/NT/2000/ME/Server 2003/XP Device Server configuration/management tool. You must install the DeviceManager from the CD-ROM included with the Device Server. Through the DeviceManager, you can:

- assign an IP address to new Device Servers.
- perform firmware updates.
- create configuration files, which can be immediately downloaded to the Device Server.
- save configuration files locally in the DeviceManager's native binary format or to a text file. The text configuration file can be edited with a text editor.
- open a session to a Device Server and import a (saved) configuration file.
- view statistics for a Device Server.
- download custom files, such as new terminal definitions and a custom language file.
- download a configuration file to multiple Device Servers.

You can use the DeviceManager as a stand-alone application to create configuration files that can be saved locally or you can use the DeviceManager to open a session to a Device Server to actively manage and configure it.

See Chapter 5***, Using the DeviceManager*** on page 51 for information on configuring/managing the Device Server with DeviceManager.

WebManager

The WebManager is a web-browser based method of configuring/managing a Device Server.

To access a Device Server through the WebManager, open up your web browser and type in the IP address of the Device Server that you want to manage/configure. A login screen will appear. Type in the Admin password.

Using the WebManager

The Server Configuration window is displayed after you first log on. The running Device Server configuration is displayed in the WebManager. You navigate through the different configuration windows by selecting the configuration window from the drop-down options in the upper-lefthand corner of the browser.

When you have completed all the changes to a configuration window, click the **Submit** button. After you make all your configuration changes, click the **Save to FLASH** button. If you want your changes to take effect immediately, click the **Reboot** button. You can make changes to a line, **Submit** them, and then click the **Kill Line** button to test the changes immediately; however, if you do not click the **Save to FLASH** button, your changes will be lost the next time the Device Server reboots. After you click the **Reboot** button, you will need to reconnect and login to the Device Server.

Note: Use the WebManager's drop-down menus to navigate through the WebManager. Do not use the browser's Back button.

CLI

The Command Line Interface (CLI) is a command line option for Device Server configuration/management and user access. See Chapter 6*, **Command Line Interface*** on page 87 for a full explanation of how to use the CLI.

Menu

The Menu is a window-oriented Device Server configuration and user access option. To manage the Device Server, you will also need to use the CLI, WebManager, or DeviceManager, as you cannot download or upload files to the Device Server through the Menu.

Accessing the Menu

Menu access is available to any user whose Line Service is set to DSLogin, and whose User Service is set to DSPrompt. What the user sees depends on what the User Level is set to:

- **Menu**—Users with **User Level Menu** will only see the sessions that have been set up for them. They can start predefined sessions, kill (stop) a running session, resume a session, and logout of the Device Server.
- **Restricted**—Users with **User Level Restricted** can basically perform the same tasks as a Menu user, except that they have the option of performing these tasks via the Menu or the CLI.
- **Normal**—Users with **User Level Normal** can do everything a Restricted user can do, plus start a free session (connecting to any host on the network), set up their own user parameters (sessions, password, language, hotkey prefix), define their terminal, and become the Admin user (if they know the Admin password).
- **Admin**—Users with **User Level Admin** (not the Admin user), have complete access to the Device Server, the same as the Admin user. Through the Menu program, the Admin level user can configure the Device Server, although there are several tasks that can only be done in the CLI, such as downloading and uploading files and saving the configuration to FLASH.

Menu Conventions

You select an option from the Menu by using the keyboard up and down arrows to navigate the list. 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. 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**. 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.

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 **l** (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

If you have a DHCP/BOOTP server and the Device Server's Server Service DHCP/BOOTP is enabled, the Device Server can obtain its IP address and several configuration parameters from the DHCP/BOOTP server when it boots up. However, you must use another method for creating the configuration file, like the DeviceManager, WebManager, or the CLI. See ***DHCP/BOOTP Parameters*** on page 50 for more information on the DHCP/BOOTP parameters that can be set for the Device Server.

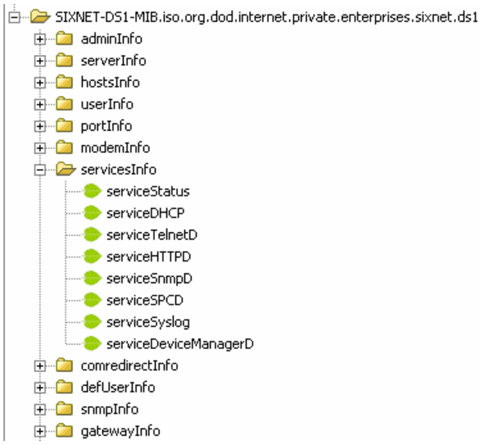
When DHCP/BOOTP is enabled and there is a DHCP/BOOTP server within the network, the IP Address obtained from DHCP/BOOTP will always override the Device Server's configured IP Address when the Device Server is rebooted.

SNMP

Before you can configure/manage the Device Server using SNMP, you need to set the Device 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 Device Server before connecting with the SNMP manager to make your changes take effect).

Once the IP address and user/community have been set, load the file from the Device Server CD-ROM into your SNMP manager.

Connect to the Device Server through your SNMP manager using its IP address to configure/manage the Device Server. Expand the **SIXNET-DS1-MIB** folder to see the Device Server's parameter folders. Below is an example of the configurable parameters under the **ServicesInfo** folder.



```
SIXNET-DS1-MIB.iso.org.dod.internet.private.enterprises.sixnet.ds1
  adminInfo
  serverInfo
  hostsInfo
  userInfo
  portInfo
  modemInfo
  servicesInfo
    serviceStatus
    serviceDHCP
    serviceTelnetD
    serviceHTTPD
    serviceSnmpD
    serviceSPCD
    serviceSyslog
    serviceDeviceManagerD
  comredirectInfo
  defUserInfo
  snmpInfo
  gatewayInfo
```

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 Device 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 Device 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 Device 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 Device Server.

4 Configuring the Device Server

Introduction

This chapter provides general information about configuring the Device Server for your production environment. Although this chapter is not specific to any configuration method, there should be enough information that you can apply the information to any of the configuration methods.

When you are configuring the Device Server, remember that none of your configuration changes will be permanent until you submit/apply your changes, save to FLASH, and reboot the Device Server.

Configuring the Device Server

General Device Server Configuration

At this point, you should already have assigned the Device Server an IP address. Therefore, you have your choice of how to configure the Device Server; using the DeviceManager, WebManager, Menu, CLI, or SNMP.

Device Server Services

In order to be as flexible and accessible as the Device Server is, it can run several predefined daemon and client applications. The Device Server can run the following daemon applications:

- TelnetD
- SPCD (the COMredirect daemon)
- DeviceManagerD
- HTTPD
- SNMPD
- ModbusD

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

The following client applications can run on the Device Server:

- Syslog
- DHCP/BOOTP

If you do not have a DHCP/BOOTP server in your network, we recommend that you keep the DHCP/BOOTP service disabled to speed up Device Server reboots (otherwise, the Device Server waits for a DHCP/BOOTP packet until it times out, about a minute, on a reboot).

By default, all daemon and most client applications (except DHCP/BOOTP) are enabled and running on the Device Server.

COMredirect

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. 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 Device Server. You must be running the COMredirect daemon on the host that is accessing the serial device for this to work. See COMredirect on page 133 for more information about the COMredirect utility.

Hardware Configuration

Configure the ethernet interface that is connecting the Device Server to the LAN and the serial cable that is connecting the Device Server to the serial device.

Ethernet Connection

You need to know the ethernet interface speed and duplex as follows, unless you are using the Auto detect option:

- 10 Mbps half or full duplex
- 100 Mbps half or full duplex

Serial Connection

You also need to know the serial interface specifications as follows:

- EIA-232 and its speed
- EIA-422 and its speed
- EIA-485 and
  - its speed
  - half duplex with/without echo suppression or full duplex
  - TX driver control is automatic or RTS

Other

The most important thing to keep in mind when configuring the hardware parameters is to make sure that they are consistent with the serial device you have connected to the port. So, if you are connecting to a modem that sends out a DSR signal, you probably want to turn the **Monitor DSR** option on. Following is a list of just some of the other hardware configuration options:

- Data Bits—5 to 8
- Stop Bits—1, 1.5, 2
- Monitor DSR—on, off
- Monitor DCD—on, off
- Parity—None, Odd, Even, Space, Mark
- Flow—Software, Hardware, or None

Modbus Configuration

This sections provides a brief overview of the steps required to configure a Device Server for your Modbus environment. You can read the ***Modbus Gateway Settings*** on page 36 and ***Modbus Line Settings*** on page 37 sections for more specific information about the Modbus settings.

Overview

Configuring a Master Gateway

To configure a Master Gateway (Modbus Master resides on the serial side of the Device Server), do the following:

1. Verify that the default Modbus Gateway settings (the settings to the Slave Gateway do not apply here) in the Server section work in your environment; if they don’t configure as required.
2. Set the **Line Service** parameter to **Modbus Master** for the Line connected to the Modbus serial Master.
3. In the Modbus Master settings, map the Modbus TCP Slave’s IP addresses and their UIDs that the Modbus serial Master will attempt to communicate with.

Configuring a Slave Gateway

To configure a Slave Gateway (Modbus Master resides on the TCP/Ethernet network), do the following:

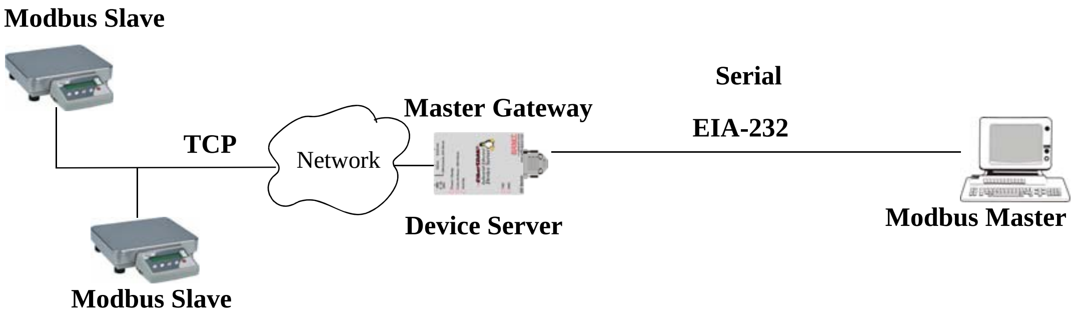
1. Verify that all the default Modbus Gateway settings in the Server section work in your environment; if they don’t configure as required.
2. Set the **Line Service** parameter to **Modbus Slave** for the Line connected to the Modbus serial Slaves.
3. In the Modbus Slave settings, specify the Modbus Slave UIDs that the Modbus TCP Master will attempt to communicate with.

Modbus Gateway Settings

The scenarios in this section are used to illustrate how the Modbus Gateway settings are incorporated into a Modbus device environment. Depending on how your Modbus Master or Slave devices are distributed, the Device Server can act as both a Slave and Master Gateway(s) on a multiport Device Server or as either a Slave or Master Gateway on a single port Device Server.

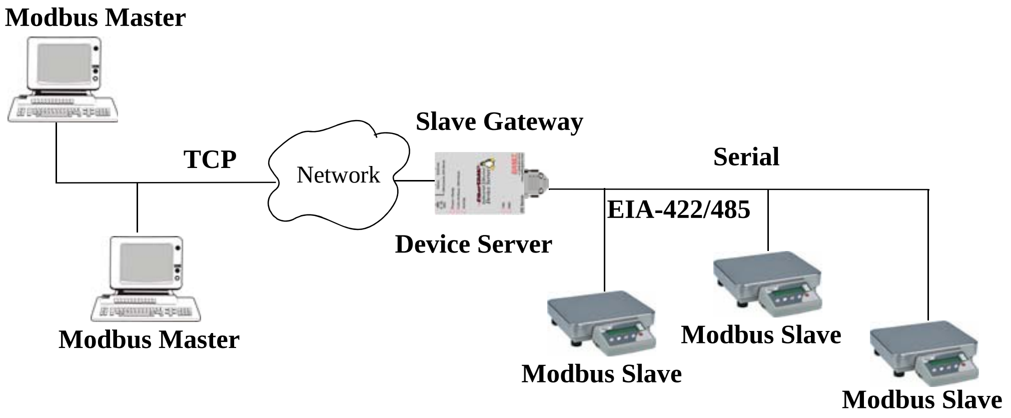
Modbus Master Gateway

The Device Server acts as a Master Gateway when the Modbus Master resides on the serial side of the Device Server. Each Modbus Master can communicate to UIDs 1-247.



Modbus Slave Gateway

The Device Server acts as a Slave Gateway when the Modbus Master resides on the TCP/Ethernet network and the Modbus Slaves reside on the serial side of the Device Server. Note that there is only one Slave Gateway for the Device Server. You can define only one Slave Gateway for the Device Server, although multiple lines/ports can participate as part of that gateway (depending on how you configure the **Line Service** settings).

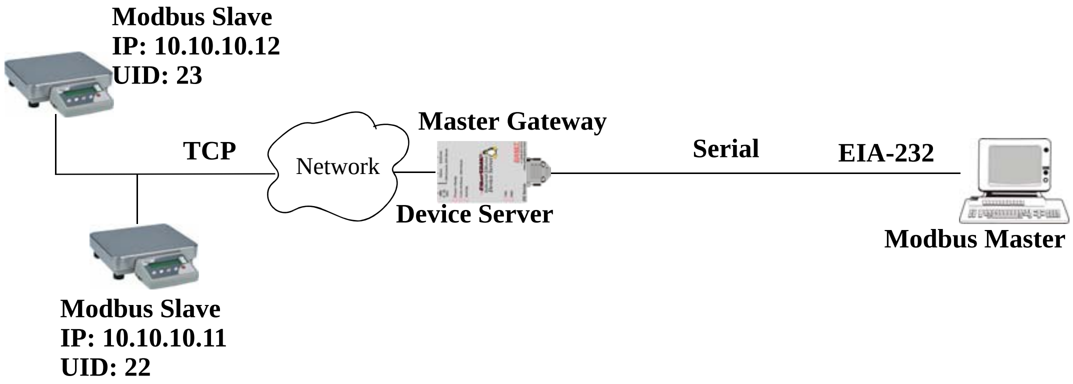


Modbus Line Settings

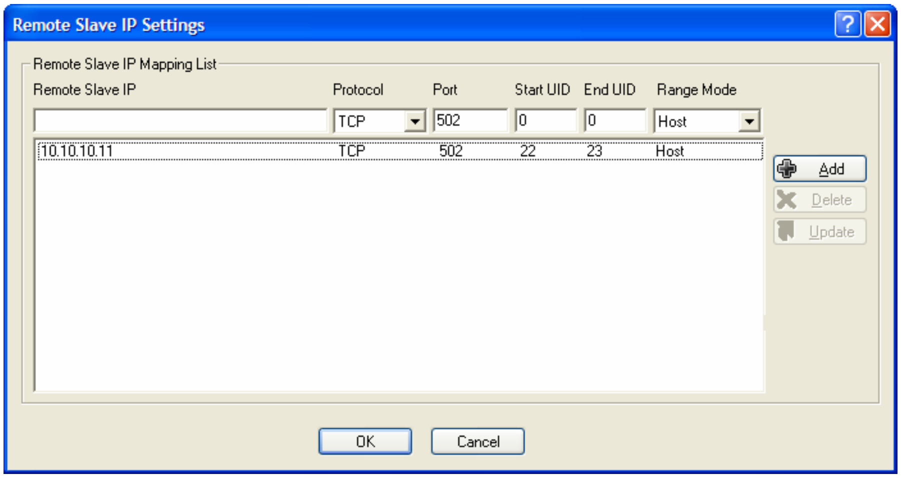
Modbus Master Settings

When you have Modbus Masters on the serial side of the Device Server, configure the Line as a Modbus Master. You must configure the Modbus TCP Slaves (we term these as Remote Slave IP Mappings) on the TCP/Ethernet side so the Device Server can properly route messages to the appropriate UIDs configured for those remote Modbus TCP Slaves.

For example, the following describes the setup configuration steps that you would use to configure a Modbus environment on a Device Server, where the Modbus Master resides on a serial port/line of the Device Server. This scenario assumes two things, that the **Service ModbusD** (the Modbus daemon) is enabled and that the default **Modbus Gateway** settings have not been changed. The Modbus Master communicates with Modbus Slaves that reside on the TCP/Ethernet network. The Device Server will act as a Master Gateway for the Modbus serial Master and allow it to communicate to the remote Modbus TCP Slaves.



When the Modbus Master is communicating with the TCP/Ethernet Modbus Slaves, the Line/port that the Modbus Master is attached to must be configured with a **Line Service** of **Modbus Master**. By configuring the Remote Slave IP settings as:


Remote Slave IP Settings

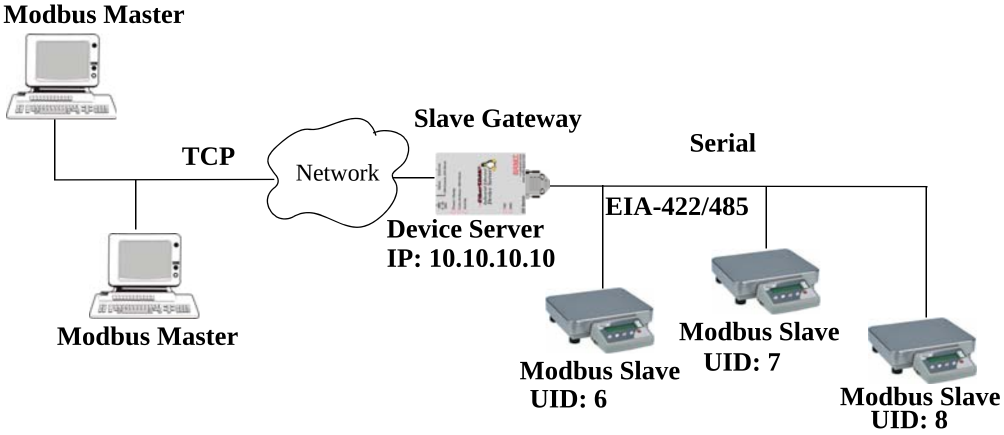
Remote Slave IP Mapping List

Remote Slave IP	Protocol	Port	Start UID	End UID	Range Mode
	TCP	502	0	0	Host
10.10.10.11	TCP	502	22	23	Host

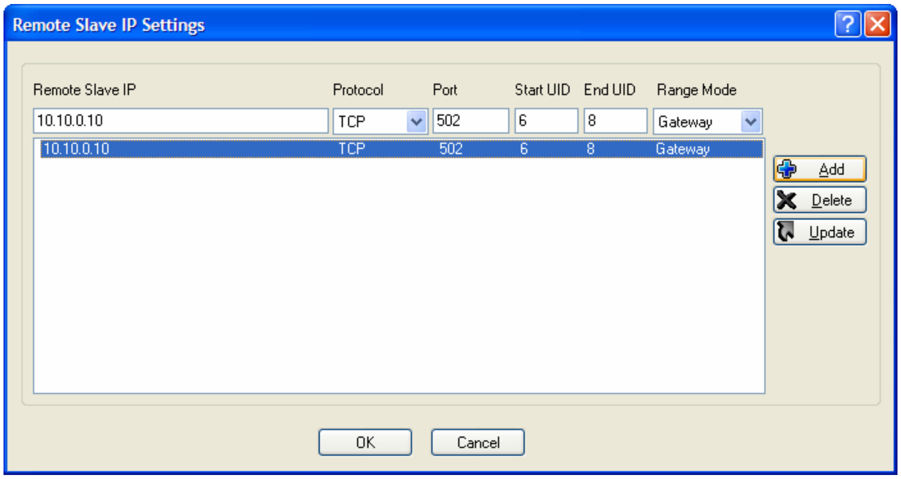
The Device Server will send a request and expect a response from a Modbus Slave with an IP Address of 10.10.10.11 on Port 502 with UID 22 and from Modbus Slave with and IP Address of 10.10.10.12 on Port 502 with UID 23 (remember when **Range Mode** is set to **Host**, the Device Server increments the last octet of the IP address for each UID specified in the range).

Modbus Slave Settings

When you have Modbus Slaves on the serial side of the Device Server, configure the Line as a Modbus Slave. There is only one Slave Gateway in the Device Server, so all Modbus serial Slaves must be configured uniquely for that one Slave Gateway; all Modbus serial Slaves must have unique UIDs, even if they reside on different serial ports, because they all must be configured to communicate through the one Slave Gateway.



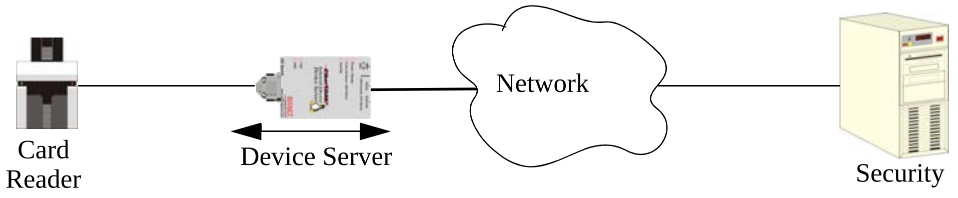
To communicate with the Modbus Slaves on the serial side of the Device Server, the Device Server must be configured to be a Slave Gateway. The Modbus Slaves on a serial port attached to the Device Server must be connected to a Line/port that is configured for the **Line Service** of **Modbus Slave**. To communicate with the Modbus Slaves on the serial port configured as part of a Slave Gateway, the Remote Slave IP settings are configured as:


Remote Slave IP Settings

Remote Slave IP	Protocol	Port	Start UID	End UID	Range Mode
10.10.0.10	TCP	502	6	8	Gateway
10.10.0.10	TCP	502	6	8	Gateway

Machine To Machine Connections

If you are using the Device Server to connect two hosts, allowing data to flow freely between them, you just need to configure the **Server** and the **Line** (no **User** required). In the following example, the serial device is a security Card Reader that needs to transmit and receive information to/from a host on the network that maintains the Card Reader's application every time an employee uses an access card to attempt to gain entry to the company.



After configuring the **Server** parameters (**Server Name**, **IP Address**, **Ethernet** and **Serial** interfaces, etc.), the **Line Service** is set to **Sil Raw**, which creates an automatic, continuous connection between the Card Reader and its associated application on the Security host (though the Device Server), by specifying the Security host name (which must already be configured in the Device Server's Host Table) and TCP/IP port number. Therefore, the Card Reader can make a request to the Security host card reader application for employee verification, also logging access time, employee name, etc., and the Security host application can send back a code that does or does not unlock the door.

Users Connecting to Serial Devices

For a user to connect to the serial device connected to the Device Server from the LAN, the **Line Service** must be set to **Rev Telnet**. The user will either access the serial device directly or go through the Easy Port Access Menu, depending on the **User Level** setting.

Users who are **Level Admin** or **Normal** will access the serial device directly; the user must connect to the Device Server's IP address and port number (the **DS Port** parameter). The user will be asked to login with a user name and password; if this is successful, the user is automatically connected to the serial device.

Users who are **Level Restricted** or **Menu** can access the serial device through the Easy Port Access Menu, which displays the line number and name and a logout option; the user just needs to connect to the Device Server's IP address. The user will be asked to login with a user name and password; if this is successful, the Easy Port Access Menu is displayed.

Users Connecting to the LAN

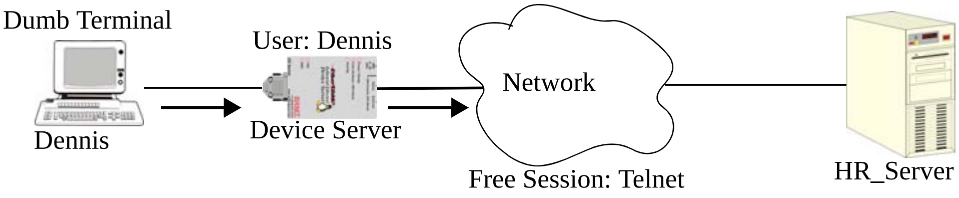
For a user to connect to the LAN through the Device Server from a serial device, the **Line Service** can be set to any **Direct** or **Silent** setting, plus **Bidir** or **DSLogin**.

User accounts should be created when:

- authentication is being done locally by the Device Server.
- you want to create predefined sessions for a user to limit that user's access to the network.

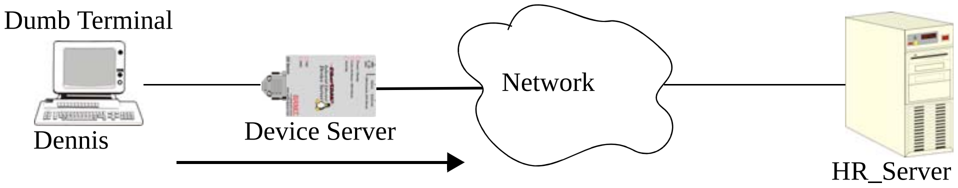
Connecting To the Device Server

When a user connects to the Device Server, that user is authenticated and is usually set up with predefined sessions or given the opportunity to configure a **Free Session** to access any host using any protocol (must have a **Level** of at least **Normal** to configure a **Free Session**). In this example, the user must have a **Line** and **User Service** of **DSLogin** and **DSPrompt**, respectively. So, user Dennis is authenticated by the Device Server and then chooses to configure a **Free Session** to the HR_Server using the Telnet protocol (Dennis could have attempted to access any host on the network).



Connecting Through the Device Server

When a user connects through the Device Server, that user is authenticated and is usually set up with a **User Service** that, once authentication is completed successfully, passes the user onto the specified host. Therefore, the **Line Service** is set to **DSLogin** and the **User Service** is set to whatever protocol the user will use to access the host; in this example, the **User Service** is set to **Dir Telnet**. When **User Service Dir Telnet** is selected, the IP address of the HR_Server is specified as the target Host IP. User Dennis will always have to log into the same server with this configuration.



Setting Up Lines

Line and port is often used interchangeably. They are almost the same, that is, each line has an associated port number (Line 1 is port 10001 by default).

How you set up a line is really determined by the device that is connected to the line. This section goes over some of the common ways a line is used and things that you will want to keep in mind when configuring the line.

DSLogin

When you configure the **Line** for **DSLogin**, users connecting to the Device Server will have to go through some form of authentication, either local or remote authentication. Regardless of whether a user has been configured in the User table (local authentication) or is inheriting the Default User's attributes (remote or Guest authentication), when a **User Service** is selected (other than **DSprompt**), that connection (**Telnet**) will inherit the connection settings defined for **DSLogin**.

Direct/Silent/Reverse Connections

Direct connections bypass the Device Server, enabling the user to log straight into a specific host. A direct connection is recommended where a user logging in to the Device Server is not required. It is also recommended where multiple sessions are not a requirement. Direct connections require user interaction: the message **`Press return to continue`** is displayed on the user's screen and the session to the host is not initiated until **Enter** is pressed, after which the host login prompt is displayed. The message is redisplayed on logout.

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 redisplays 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.

Reverse connections enable a host on the network to establish a connection through the Device Server port to a serial device.

Virtual Modems

Vmodem is a feature of the Device Server that provides "modem like" communication between two Device Servers on a network or between a Device Server and a host. This feature behaves like two modems connected across a telephone line. Typically, you use the **Vmodem** feature when you have multiple devices communicating with a central site. With just a single SIXNET Device Server at each end of the network, you don't need to use multiple modems, avoiding the associated costs of calls and connections.

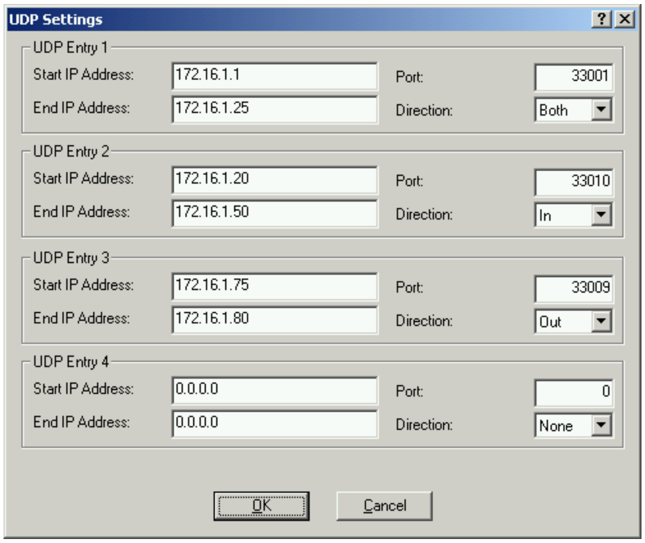
The data is sent in raw format from the virtual modem and can be received by another Device Server or a host. This data can be sent automatically using the **Monitor DSR** option and then configuring the host and port number of the receiver; if the receiving side is also a Device Server, set the **Line Service** to **Rev Raw** or **Vmodem** (**Rev Raw** if the Device Server is only receiving, **Vmodem** to initiate bidirectional data flow) and the Device Server port that the data is coming in on (this should match the port number on the sending Device Server). Or, you can 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 **`ATD12334234310001`**, without any punctuation.

BIDIR

When you configure **BIDIR**, you are creating a bidirectional raw connection, meaning that the connection can be initiated from either the ethernet or serial side.

UDP

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



UDP Entry 1
Start IP Address: 172.16.1.1
End IP Address: 172.16.1.25
Port: 33001
Direction: Both

UDP Entry 2
Start IP Address: 172.16.1.20
End IP Address: 172.16.1.50
Port: 33010
Direction: In

UDP Entry 3
Start IP Address: 172.16.1.75
End IP Address: 172.16.1.80
Port: 33009
Direction: Out

UDP Entry 4
Start IP Address: 0.0.0.0
End IP Address: 0.0.0.0
Port: 0
Direction: None

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

- **UDP Entry 1**

  All hosts that have an IP address that falls within the range of **`172.16.1.1`** to **`172.16.1.25`** and listen to **Port `33001`** will receive UDP data from the serial device. The serial device will only receive UDP data from the hosts in that range with a source **Port** of **`33001`**.
- **UDP Entry 2**

  All UDP data received from hosts that have an IP address that falls within the range of **`172.16.1.20`** to **`172.16.1.50`** and **Port `33010`** will be sent to the serial device. The Device Server will not send any data received on its serial port.
- **UDP Entry 3**

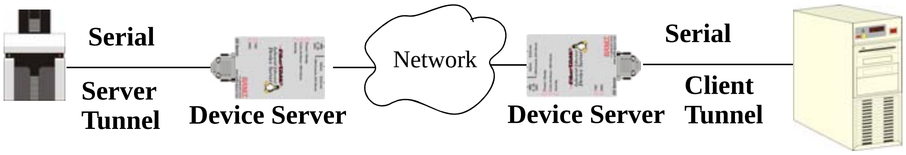
  All hosts that have an IP Address that falls within the range of **`172.16.1.75`** to **`172.16.1.80`** and who listen to **Port `33009`** will receive UDP data from the serial device. No UDP data will be sent to the serial device.
- **UDP Entry 4**

  This entry is disabled since **Direction** is set to **None**.

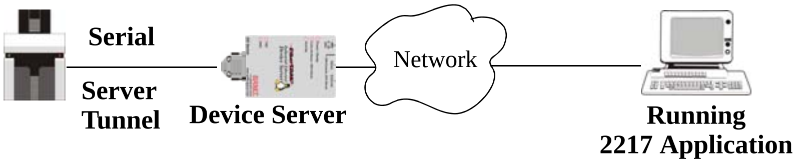
If **Direction** is set to **In** or **Both**, and **Port** is set to **`0`** (zero), the Device Server will learn a host IP Address and Port number based on the first UDP packet it receives and will then only send and/or accept UDP data from that host.

Serial Tunnel Settings

The purpose of the serial **Line Service Client/Server Tunnel** is to allow two Device Servers that are connected back-to-back over Ethernet to virtually link two serial ports, based on RFC 2217. The serial device that initiates the connection is the **Client Tunnel** and the recipient is the **Server Tunnel**, although once the serial communication tunnel has been successfully established, the tunnel will stay connected and communication can go both ways.



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



The port signals will also follow the signals on the other port. If one port receives DSR then it will raise DTR on the other serial port. If one port receives CTS then it will raise RTS on the other port.

Setting Up Users

You can create up to four users, in addition to the Admin user (who cannot be deleted).

A user can even represent a device, like a barcode or a card swipe device, that you want to be authenticated.

User Accounts

When a serial device (like a dumb terminal or a barcode reader) is trying to access a host through the Device Server, you will need to configure user accounts when users:

- are authenticated by the Device Server and then connect to a host.
- want a single or multiple session(s) on a host; here they initially login to the Device Server before starting that session. The Device Server is used to configure and start the session.

When a host is accessing a serial device (like a modem or a server), you will need to configure user accounts where users:

- are using a reverse telnet connection to manage a UNIX server or a router.

User Levels

There are four **User Levels**: **Admin**, **Normal**, **Restricted**, and **Menu**. Setting up users is only necessary when the users are actually connecting to the Device Server. Oftentimes, the Device Server is used as a gateway to a network and the user never actually logs into the Device Server itself. Users who do log into the Device Server (**Line Service** set to **DSLogin** and **User Service** set to **DSPrompt**) will have to navigate by either the Menu or CLI (except for users with **Menu** privileges, who can only use the Menu).

- **Admin**—Users with **Admin** privileges have full administrative access to the SIXNET Device Server. This is not the same as the Admin user, but has equal authority (the Admin user is a permanent, factory-set user on the SIXNET Device Server).
- **Normal**—Users with **Normal** privileges have access to the Sessions menu and associated CLI only. They can start sessions, define and predefine sessions, and can change their own user environment.
- **Restricted**—Users with **Restricted** privileges have access to a restricted Sessions menu and associated CLI; they can only open sessions predefined for them by the Admin user, but not alter their own environment or sessions. Predefined sessions can also be configured to start automatically at login.
- **Menu**—Users with **Menu** privileges have access to predefined session. All other functionality is unavailable.

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

Sessions

Sessions are defined for users who are coming in through a serial device going to a host on the LAN.

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

Multiple sessions can be run simultaneously on the same host or on different hosts. Users can switch between different sessions and also between sessions and the Device Server using hotkey commands.

Users with **Admin** or **Normal** privileges can define new sessions and connect through them, even configure them to start automatically on login to the Device Server. **Restricted** and **Menu** users can only start sessions predefined for them by the Admin user.

You can configure the User access rights to the port, such as **Read/Write** (RW) or **Read Input** (RI).

Users From LAN to Device Server to Serial Device

Easy Port Access Menu

The Easy Port Access Menu is displayed when a **Restricted** or **Menu** level user logs into the box from the Ethernet side (**Line Service** set to **Rev Telnet**) to access a serial device. The Easy Port Access Menu displays the line number, line name, line protocol, and a logout option. You can only access the line if it has the same connection protocol as the one you used to log into the Device Server. So, if you used SSH to log into the Device Server and the **Line Service** is set for **Rev Telnet**, you will not be able to access the serial device connected to that line.

Configuring Network Options

Hosts

This is probably one of the first Device Server options you want to configure, since so many other configuration options require a preconfigured host. You can use any host name you want, since the host name is used only by the Device Server. You can configure up to 20 hosts using IPv4 or IPv6 internet addresses.

Gateways

Gateways are hosts that connect Local Area Networks (LANs) together. If you want to access a host that isn't on your local network, you will be connected via a gateway. Gateways route data via other gateways until the destination local network is reached. There are three types of gateways:

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

You can specify up to twenty gateways.

Syslog

The system log is sent to the specified host. You can configure a primary and secondary host for the syslog information and specify the level for which you want syslog information sent.

SNMP

If you are using SNMP to manage/configure the Device 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 Device Server; this can be done in the DeviceManager, WebManager, CLI, or Menu. You must then load the sixnet-ds1.MIB (found on the CD-ROM packaged with the Device Server) file into your SNMP manager before you connect to the Device Server.

Configuring Time

The Device Server has an internal clock that can be set, but it will be reset during a reboot or a power outage.

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 Device Server and select the **Language** option of **Customlang** (custom language), making the Menu, CLI, and WebManager field labels display in your language.

You can view Menu, CLI, or WebManager 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 Device Server and is not overwritten by your new language. Each user logged into the Device 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 Device Server, so the Menu, CLI and WebManager fields appear in another language, do the following:

1. Open the supplemental CD and identify the language file, either **`ds_French.txt`** or **`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 Device Server or, configure as necessary, TFTP in the Device Server.
4. In the CLI of the Device Server, enter the host IP address and file name; for example,

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

   Do *not* enter a drive letter! Also, the path and/or file name must begin with the forward slash (/) character.

   The Device Server will download the language file via TFTP.
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 Device 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.

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 Device 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 Device 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, CLI, or WebManager.
- 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 Device 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, CLI, or WebManager.

If you are already using one of the supplied languages, French or German, you probably want to update the language file in the Device Server. Until you update the Device 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, CLI, or WebManager in English.

Downloading Terminal Definitions

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

If you are not using, or cannot emulate, any of these terminal types, you can add up to three additional terminal definitions to the Device 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 TFTP enabled.
2. Configure TFTP in the Device Server as necessary.
3. Download the new terminal definition to the Device Server as **Term1**, **Term2**, or **Term3**.
4. In the **Line** configuration, select the **Terminal Type Term*x*** 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 > term`***n* 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 Device 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.

TFTP Configuration

TFTP can be configured for two unique transfer operations:

1. Between the DeviceManager and a Device Server. This configuration is accessed by selecting Tools, Options from the DeviceManager's tool bar. You can specify the number of times the DeviceManager's TFTP server retries a file transfer to a Device Server, how long the TFTP process will wait (timeout) before retrying to transfer a file, and the UPD port that will be used for the file transfer between the DeviceManager and the Device Server. (DeviceManager only.)
2. Between the Device Server and a host. This configuration is accessed by selecting Network, TFTP in the DeviceManager, by typing **`set server tftp`** in the CLI, by selecting **Network Configuration**, **TFTP** from the Menu, by selecting **ServerInfo**, **tftpRetry** and **tftpTimeOut** in the SNMP MIB, or by selecting **Network**, **TFTP** in the WebManager. You can configure the number of times the Device Server's TFTP client retries a file transfer to a host and how long the TFTP process will wait (timeout) before retrying to transfer a file.

You must have a TFTP server running on any host that you are uploading or downloading files to/from. If you are using the DeviceManager and transferring a local file to a Device Server, you still need to have a TFTP server running on your PC. When you specify the file path, the path must be relative to the default path set in your TFTP server software (do not use drive letters in the file path).

Resetting Configuration Parameters

You can reset the Device Server to its factory settings through any of the following methods:

- You can push in the recessed button at the back of the Device Server hardware
- DeviceManager, select **Tools**, **Reset to Factory Defaults**
- CLI, at the command line type, **`reset factory`**
- WebManager, click the **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 Device Server to the factory defaults
- have another user that has **admin** level rights, if one is already configured, reset the Admin password

DHCP/BOOTP

You can use DHCP/BOOTP to perform the following actions on a single or multiple Device 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 Device Server's configuration in one DHCP/BOOTP file, rather than configure each Device Server manually. Another advantage of DHCP/BOOTP is that you can connect a Device Server to the network, turn on its power, enable DHCP/BOOTP, 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 Device Server from the HTTP WebManager. Values are **`on`** or **`off`**.
- **SECURITY**—Restricts Device Server access to devices listed in the Device 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/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.

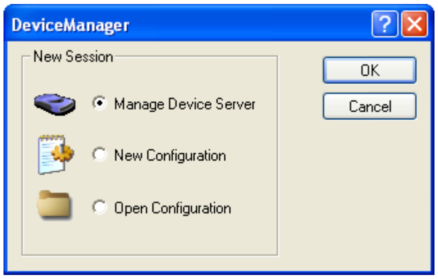
5 Using the DeviceManager

Introduction

This chapter provides information about configuring/managing the Device Server using the DeviceManager. It is assumed that the DeviceManager has already been installed; if you still need to install the DeviceManager, see ***Using DeviceManager*** on page 23.

Starting a New Session

When you start the DeviceManager application, the New Session window is displayed.

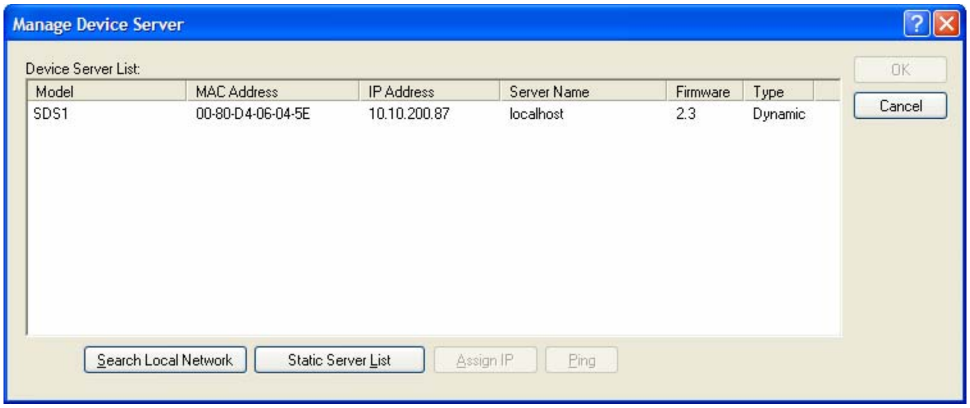


You can choose:

- **Manage Device Server**—Connect to a Device Server to manage/view it.
- **New Configuration**—Create a new Device Server configuration.
- **Open Configuration**—Open an existing configuration file.

Managing a Device Server

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



Device Server List:

Model	MAC Address	IP Address	Server Name	Firmware	Type
SDS1	00-80-D4-06-04-5E	10.10.200.87	localhost	2.3	Dynamic

If you want to connect to a Device Server to manage/configure it, or assign a temporary IP address to a Device Server, select **File**, **New Session** and the **Manage Device Server** radio button. If you want to create a new or edit an existing configuration file, select **File**, **New Session** and the **New Configuration** or **Open Configuration** radio button.

Populating the Device Server List

The first time you start the DeviceManager, the **Manage Device Server** window will be empty. To add Device Servers to the Device Server **List**, you can do either of the following:

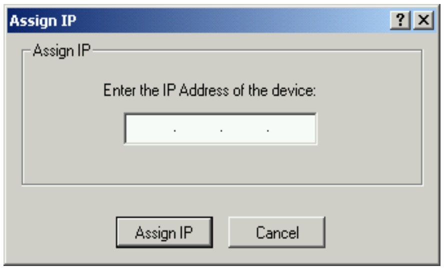
- Click the **Search Local Network** button. This searches the local network segment and automatically displays any Device Servers it finds. Any Device Servers found by this method will be displayed in **Type** column as **Dynamic**. Once you close the DeviceManager, any Device Servers that were displayed as **Dynamic** will not be there until you click the **Search Local Network** button again.
- Click the **Static Server List** button to add Device Servers to the Device Server **List** permanently. This also allows you to add Device Servers that are not found on the local network segment with the **Search Local Network** button. To connect to a Device Server that is not in the Device Server List and resides outside the local network, see ***Adding/Deleting Static Device Servers*** on page 53.

For more information about managing a Device Server, see ***Managing a Device Server*** on page 55.

Assigning a Temporary IP Address to a New Device Server

If your network does not use DHCP/BOOTP, you can temporarily assign an IP address to a Device 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 Device Server, do the following:

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

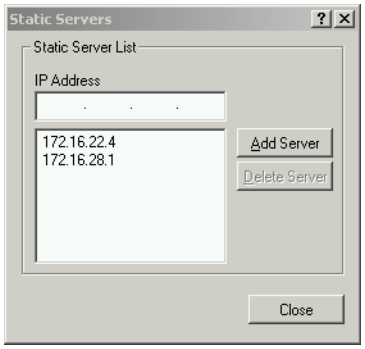


3. Type a valid temporary IP address into the address field and click the **Assign IP** button.
4. Double-click the Device Server in the Device Server **List**. If this is the first time you are accessing the Device Server, type in the factory default Admin password, **`superuser`**, and click **OK**. The DeviceManager will display a window indicating that it is trying to authenticate and connect you on the Device Server.
5. If the authentication and connection are successful, the Server Info window is displayed. You are now ready to configure the Device Server. If authentication was unsuccessful, try to connect to the Device Server again; you probably mistyped the password for the Admin user.

For more information about managing a Device Server, see ***Managing a Device Server*** on page 55.

Adding/Deleting Static Device Servers

To permanently add or delete a Device Server to/from the Device Server **List**, select the **Static Server List** button. The following window is displayed:

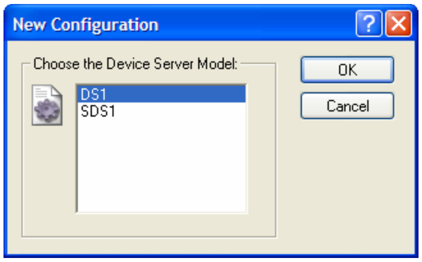


172.16.22.4
172.16.28.1

To permanently add a Device Server to the Device Server **List**, type in the IP address of the Device Server and click the **Add Server** button. To permanently delete a Device Server from the Device Server **List**, select the Device Server's IP address and click the **Delete Server** button.

Creating a New Device Server Configuration

If you selected the **New Configuration** radio button, the New Configuration window is displayed.



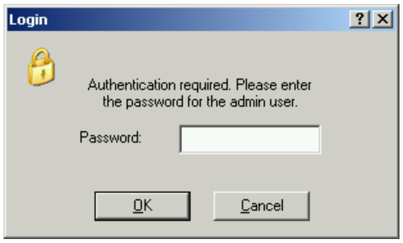
Select the Device Server model for which you want to create a new configuration file.

Opening an Existing Configuration File

If you selected the **Open Configuration** radio button, a browse window is opened so you can select the configuration file you want to edit. Device Server configuration files can be in the Device 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.

Connecting to a Device Server

To connect to a Device Server, double-click on the Device Server in the **Device Server List**. You will be prompted for the Admin Password.


Authentication required. Please enter the password for the admin user.

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

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

Managing a Device Server

Once you are connected to a Device Server, you can edit its configuration, download a new configuration, save the configuration to file, perform administrative tasks, and view statistics about the Device Server and its network environment.

DeviceManager Work Flow

When you connect to a Device Server, the Device Server's configuration is automatically uploaded to the Device Server. Before you make any changes to the configuration, you probably want to save the configuration locally, to make a backup file of the configuration. Use the navigation panel to select the feature that you want to edit. After you make all your changes to a configuration window, you must click the **Apply** button to submit those changes. When you have completed all of your configuration edits, select **Tools**, **Download Configuration to Unit**. If you want your changes to take effect at this point, select **Tools**, **Reboot Server**.

Creating/Editing Configuration Files

You can create and edit Device Server configuration files. When you open a new configuration file, the configuration file contains the Device Server's factory default settings.

Working With the Device Server Configuration

When you connect to a Device Server, the configuration that is saved to FLASH is automatically uploaded to the DeviceManager. It is suggested that you save the working configuration to a file as a backup precaution by selecting **Tools**, **Save Configuration to File**. You can then make any edits to the configuration and download it back to the Device Server by selecting **Tools**, **Download Configuration to Unit**. The downloaded configuration does not take effect until you reboot the Device Server by selecting **Tools**, **Reboot Server**. If you want to continue managing/configuring the Device Server, you can reconnect to the Device Server after it has been rebooted.

Working With a Local Configuration File

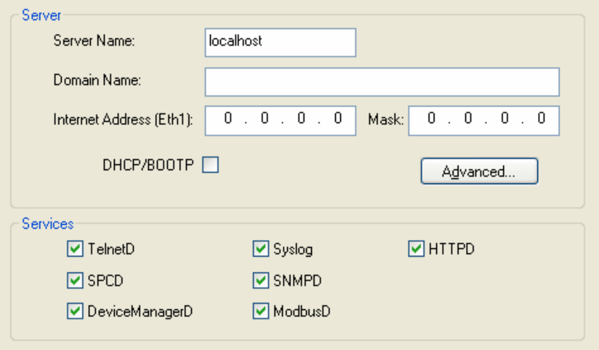
You can also connect to a Device Server and open a saved configuration file by selecting **Tools**, **Get Configuration**, **Import from File**. This configuration can then be edited or just downloaded right to the Device Server by selecting **Tools**, **Download Configuration to Unit.** The downloaded configuration does not take effect until you reboot the Device Server by selecting **Tools**, **Reboot Server**. If you want to continue managing/configuring the Device Server, you can reconnect to the Device Server after it has been rebooted.

Configuring the Server

The following sections describe how to configure the Device Server's server parameters.

Configuring the Main Server Window

When you select **Server Configuration**, **Server** from the navigation panel, the following Server window is displayed.



Server

Server Name: localhost

Domain Name:

Internet Address (Eth1): 0 . 0 . 0 . 0 Mask: 0 . 0 . 0 . 0

DHCP/BOOTP ☐

Services

☑ TelnetD ☑ Syslog ☑ HTTPD

☑ SPCD ☑ SNMPD

☑ DeviceManagerD ☑ ModbusD

Enter values in the Device Server parameters that you need for your production environment.

Server

Server Name

You must supply a name for the Device Server.

Domain Name

Unique name for your domain, your location in the global network. Like Hostname, it is a symbolic, rather than a numerical, identifier.

See ***IPv6 Network*** on page 25 for information on how to determine your IPv6 address.

Internet Address

The Device Server's unique IPv4 network IP address. If you are using the Device Server in an IPv6 network, this field can be left blank.

Mask

The number of bits in the subnet mask. For example, a subnet mask of 255.255.0.0 has 16 subnet/prefix bits. Valid values are 0-31. The default is 0. When the value is 0, the correct value is determined based on the class of the **IP Address**.

DHCP/BOOTP

DHCP/BOOTP client process in the Device Server.

Services

Services are either daemon or client processes that run on the Device Server. You can disable any of the services for security reasons. If you disable the DeviceManagerD service, you will not be able to use DeviceManager to connect to a Device Server.

TelnetD

Telnet daemon process in the Device Server on port 23.

SPCD

SPC (COMredirect) daemon process in the Device Server on port 688.

DeviceManagerD

DeviceManager daemon process in the Device Server. If you disable this service, you will not be able to connect to the Device Server with the DeviceManager application. DeviceManagerD listens on port 33812 and sends on port 33813.

HTTPD HTTP daemon process in the Device Server on port 80.

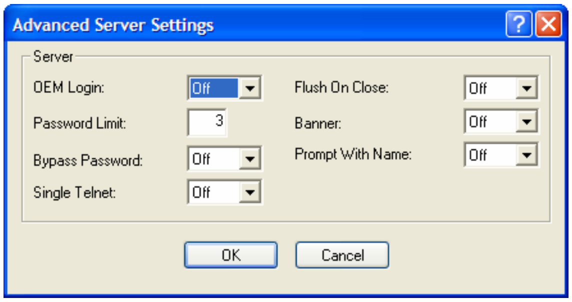
SNMPD SNMP daemon process in the Device Server on port 161.

Syslog Syslog client process in the Device Server.

ModbusD Modbus daemon process in the Device Server on port 502.

Configuring Advanced Server Settings

In the Server window, the following window is displayed when you click the Advanced button.



OEM Login: Off
Password Limit: 3
Bypass Password: Off
Single Telnet: Off
Flush On Close: Off
Banner: Off
Prompt With Name: Off

Configure the appropriate parameters:

OEM Login 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:`.

Password Limit The number of attempts a user is allowed to enter a password for a port. If this limit is exceeded, the port is disabled for 5 minutes. A user with Admin level rights can restart the port, bypassing the timeout, by issuing a kill on the disabled port. The default value is **3**.

Bypass Password When set, authorised 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**.

Single Telnet Sets all reverse connections (raw and telnet) to a one connection at a time mode. Server-side applications will get a (socket) connection refused until:

- 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

This also enables a per-connection keepalive 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 recognised by the reverse service (all connections).

Applications using Single Telnet 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; this is to allow any data sent on prior connections to be transmitted out of the serial port. Application network retry logic needs to accommodate this feature. The default value is **Off**.

Flush On Close When enabled, deletes any pending data when a port is closed; as opposed to maintaining the port to send pending data. The default value is **Off**.

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. The default is **Off**.

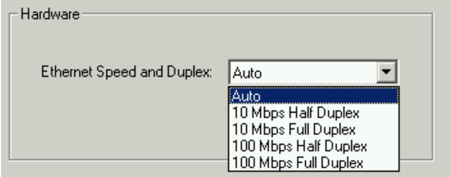
Prompt With Name Displays the **Server Name** field value instead of default product name. When enabled, the **Server Name** is displayed in the Device Server login prompt, CLI prompt, WebManager login screen, and the heading of the Menu. The default value is **Off**.

Configuring COMredirect Baud

The COMredirect Baud configuration window allows you to map the baud rate coming out of the serial host to another baud rate that will run between the Device Server and the serial device. See Appendix B, Utilities on page 133 for more information about COMredirect.

Configuring the Hardware

You need to configure the ethernet interface that you are using to connect the Device Server to the LAN.


Hardware

Ethernet Speed and Duplex: Auto

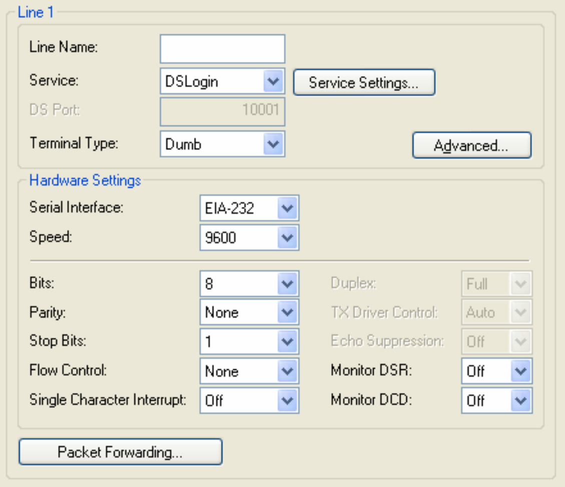
Select the appropriate option:

Ethernet Speed and Duplex Define the ethernet connection speed at one of the following:

- **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**

Configuring Lines

When you configure the Device Server **Line**, you are specifying how the port will be used and accessed. You can always make changes to **Line** parameters, click the **Apply** button, and then select **Tools**, **Kill Line** to test your changes. However, you still must select **Tools**, **Download Configuration to Unit** and **Tools**, **Reboot Server** to make your changes permanent and take effect.



Line 1

Line Name:	
Service:	DSLogin
DS Port:	10001
Terminal Type:	Dumb

Hardware Settings

Serial Interface:	EIA-232
Speed:	9600

Bits:	8	Duplex:	Full
Parity:	None	TX Driver Control:	Auto
Stop Bits:	1	Echo Suppression:	Off
Flow Control:	None	Monitor DSR:	Off
Single Character Interrupt:	Off	Monitor DCD:	Off

Configure the appropriate parameters:

Line Name

Provide a name for the line so it can be easily identified.

Service

Defines the **Line Service**, which determines how the line will be used.

See ***Service Settings*** on page 63 for more information about configuring each **Line Service**.

DS Port

The Device Server port number.

Terminal Type

Specifies the type of terminal connected to the line:

- **Dumb**
- **WYSE60**
- **VT100**
- **ANSI**
- **TVI925**
- **IBM3151TE**
- **VT320** (specifically supporting VT320-7)
- **HP700** (specifically supporting HP700/44)
- **Term1, Term2, Term3 (user defined terminals)**

Serial Interface

Specifies the type of line that is being used with the Device Server. Select either **EIA-232**, **EIA-422**, or **EIA-485**.

Speed

Specifies the baud rate of the line; keep in mind that speed is affected by the length of the cable. You can also specify a custom baud rate; valid values are 50-230400.

Bits

Specifies the number of bits in a byte. The default is **8**.

Parity

Specifies if you are using **Even**, **Odd**, or **No parity** on the line. If you want to force a parity type, you can specify **Mark** for 1or **Space** for 0.

Stop Bits

Specifies the number of stop bits that follow a byte.

Flow Control

Defines whether the data flow is handled by the software (**Soft**), hardware (**Hard**), **Both**, or **None**.

Single Character Interrupt

When enabled, causes the Device Server to process every character as it comes in, as opposed to buffering the characters before processing; this provides better latency at the expense of efficiency.

Duplex

Specify whether the line is **Full Duplex** (communication both ways at the same time) or **Half Duplex** (communication in one direction at a time).

TX Driver Control

Used with a **EIA-485** serial interface, if your application supports **RTS** (Request To Send), select this option. Otherwise, select **Auto**. Default is **Auto**.

Echo Suppression

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 **On**. The default is echo suppression **Off**.

Monitor DSR

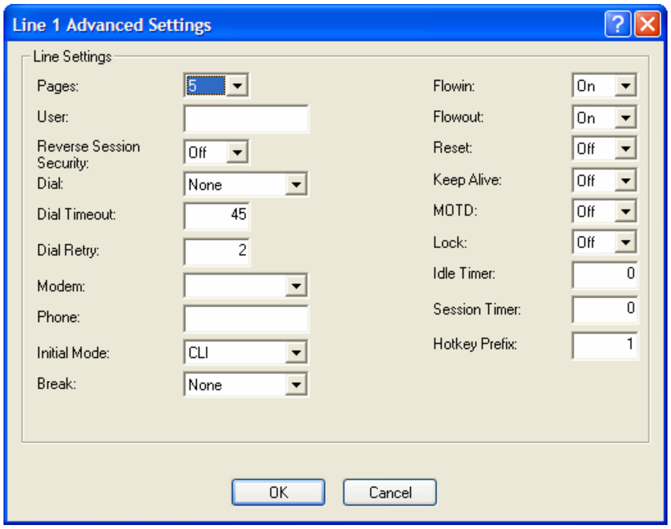
Specifies whether the RS-232 signal DSR (data set ready) should be monitored. This is used with modems or any device that sends a DSR signal. When it is monitored and the Device Server detects a DSR signal, the line service is started. Default is **Off**. If both **Monitor DCD** and **Monitor DSR** are enabled, both signals must be detected before the line service is started.

Monitor DCD

Specifies whether the RS-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 Device Server detects a DCD signal, the line service is started. Default is **Off**. If both **Monitor DCD** and **Monitor DSR** are enabled, both signals must be detected before the line service is started.

Advanced Line Settings

You can configure these advanced settings for a line.



Pages: 5
User:
Reverse Session Security: Off
Dial: None
Dial Timeout: 45
Dial Retry: 2
Modem:
Phone:
Initial Mode: CLI
Break: None
Flowin: On
Flowout: On
Reset: Off
Keep Alive: Off
MOTD: Off
Lock: Off
Idle Timer: 0
Session Timer: 0
Hotkey Prefix: 1

Configure the appropriate parameters:

Pages

For **DSLogin** line service, this is the number of video pages the terminal supports. Valid values are 1-7. The default is **5** pages.

User

For **DSLogin** line service, makes this a line that is dedicated to the specified user. Only this user will be able to log in on this line and they won’t need to enter their login name - just their password.

Reverse Session Security

Enables/disables login/password authentication, locally or externally, on reverse Telnet connections. The default is **Off**.

Dial

Determines how a modem will work on the line. If your user is remote and will be dialing in via modem or ISDN TA, set this parameter to **In**; if the Device Server is being used as a router, set this parameter to either **In**, **Out**, or **Both**, depending on which end of the link your Device Server is situated and how you want to initiate the communication.

Dial Timeout

The number of seconds the Device Server will wait to establish a connection to a remote modem. The default value is **45** seconds.

Dial Retry

The number of times the Device Server will attempt to establish a connection with a remote modem. The default value is **2**.

Modem

The name of the predefined modem that is used on this line.

Phone

The phone number to use when **Dial** is set to **Out**.

Initial Mode

Specifies the initial interface a user navigates when logging into the line; either the **Menu** or a prompt for the **CLI**. The default is **CLI**.

Break

Specifies how a break is interpreted:

- **None**—The Device Server ignores the break key completely and it is not passed through to the host. This is the default setting.
- **Local**—The Device 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 Device Server translates this into a telnet break signal which it sends to the host machine.
- **Brkintr**—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).

Flowin

Determines if input flow control is to be used. Default is **On**. This is active only when **Line Flow Control** is set to **Soft**, **Hard**, or **Both**.

Flowout

Determines if output flow control is to be used. Default is **On**. This is active only when **Line Flow Control** is set to **Soft**, **Hard**, or **Both**.

Reset

Resets the terminal type connected to the line when a user logs out.

Keep Alive

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, either ensuring the connection stays active OR causing a dropped connection condition to be recognised by the reverse raw service.

Applications using this feature need to be aware that there might be some considerable delay between a network disconnection and the port being available for the next connection attempt; this is to allow any data sent on prior connections to be transmitted out of the serial port buffer. Application network retry logic needs to accommodate this feature.

MOTD

Enables/disables the message of the day on the line.

Lock

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

Idle Timer

Enter a time period, in seconds, for which the **Idle Timer** will run. Use this timer to close a connection because of inactivity. When the **Idle Timer** expires, the Device Server will end the connection. The maximum value is 4294967 seconds (about 49 days). The default value of **0** (zero) means the **Idle Timer** will not expire, so the connection is permanently open.

Session Timer

Enter a time, in seconds, for which the **Session Timer** will run. Use this timer to forcibly close the session (connection). When the **Session Timer** expires, the Device Server will end the connection. The default value is **0** seconds so the port will never timeout. The maximum value is 4294967 seconds (about 49 days).

Hotkey Prefix

The prefix that a user types to lock a line or redraw the Menu. The default value is **hex 01**, which corresponds to **Ctrl-a** (**^a**) (hex value 02 would be Ctrl-b (^b), etc.):

- **^a l**—(Lowercase L) Locks the line until the user unlocks it. The user is prompted for a password (any password, excluding spaces) and locks the line. Next, the user must retype the password to unlock the line.
- **^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.

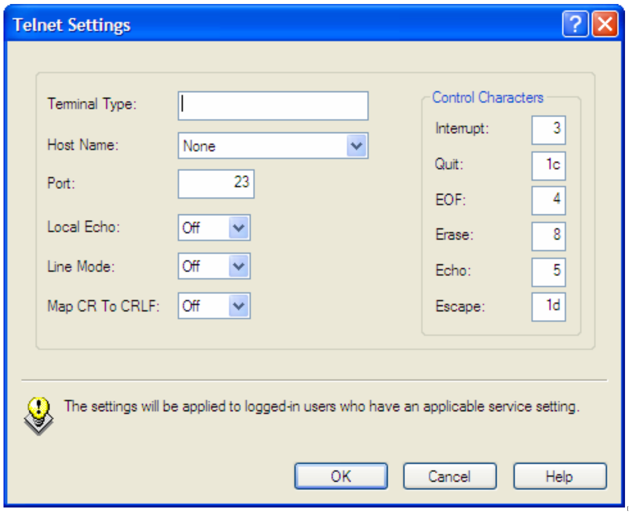
You can use the **Hotkey Prefix** key to lock a line only when the **Line Lock** parameter is **On**.

Service Settings

Line Services determine how line is defined. As a rule, when you are accessing a serial device through the Device Server, coming from the ethernet side, you want to set the **Line Service** to **Reverse Raw** or **Reverse Telnet**.

DSLogin

When the **Line Service** is set to **DSLogin**, any user accessing the Device Server will have to log into the Device Server. What happens after the user successfully logs into the Device Server is based on how the user is configured. For example, if after a successful login, the user is set to telnet to a specific host, you will want to set the Telnet parameters that will be used by the user for the telnet session (any parameters that are also available in the user's configuration are overridden by the user's definitions).



Terminal Type:

Host Name: None

Port: 23

Local Echo: Off

Line Mode: Off

Map CR To CRLF: Off

Interrupt: 3

Quit: 1c

EOF: 4

Erase: 8

Echo: 5

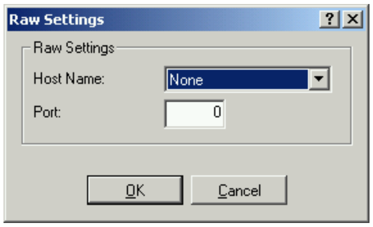
Escape: 1d

The settings will be applied to logged-in users who have an applicable service setting.

See ***Telnet Settings*** on page 64 for information on the Telnet Settings parameters.

Raw Settings

When the **Line Service** is set to **Direct** or **Silent Raw**, data is sent through the connection in its original format. This raw TCP/IP connection is initiated from the Device Server to the configured host.



Host Name: None

Port: 0

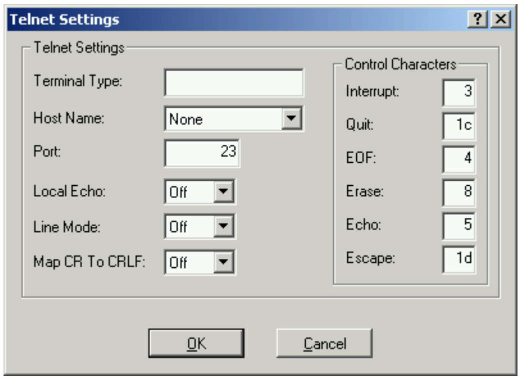
Configure the following parameters:

Host Name The name of the target host.

Port The port number the target host is listening on for incoming connections.

Telnet Settings

When the **Line Service** is set to **Direct** or **Silent Telnet**, data is sent through the connection in a telnet session. This telnet session is initiated from the Device Server to the configured host.



Terminal Type:

Host Name: None

Port: 23

Local Echo: Off

Line Mode: Off

Map CR To CRLF: Off

Interrupt: 3

Quit: 1c

EOF: 4

Erase: 8

Echo: 5

Escape: 1d

Configure the following parameters:

Terminal Type Type of terminal attached to this line; for example, ANSI or WYSE60.

Host Name The name of the target host.

Port The port number the target host is listening on for incoming connections.

Local Echo 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 only be used when **Line Mode** is **On**. Default is **Off**.

Line Mode When **On**, keyboard input is not sent to the remote host until **Enter** is pressed, otherwise input is sent every time a key is pressed. Default is **Off**.

Map CR to CRLF Maps carriage returns (CR) to carriage return line feed (CRLF). The default value is **Off**.

Interrupt

Defines the interrupt character. Typing the interrupt character interrupts the current process. This value is in hexadecimal with a default value of **3** (ASCII value **^C**).

Quit

Defines the quit character. Typing the quit character closes and exits the current telnet session. This value is in hexadecimal with a default value of **1c** (ASCII value **FS**).

EOF

Defines the end-of-file character. When Line Mode is On, entering the eof character as the first character on a line sends the character to the remote host. This value is in hexadecimal with a default value of **4** (ASCII value **^D**).

Erase

Defines the erase character. When Line Mode is Off, typing the erase character erases one character. This value is in hexadecimal with a default value of **8** (ASCII value **^H**).

Echo

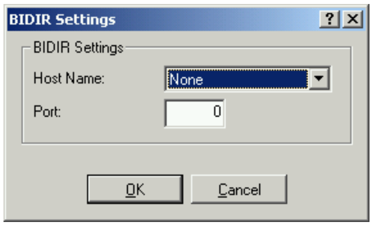
Defines the echo character. When Line Mode is On, typing the echo character echoes the text locally and sends only completed lines to the host. This value is in hexadecimal with a default value of **5** (ASCII value **^E**).

Escape

Defines the escape character. Returns you to the command line mode. This value is in hexadecimal with a default value of **1d** (ASCII value **GS**).

BIDIR Settings

When the **Line Service** is set to **BIDIR**, a bidirectional connection is created, with data flowing in both directions in its original format. This raw TCP/IP connection can be initiated from either the Device Server or the configured host.



BIDIR Settings

BIDIR Settings

Host Name: None

Port: 0

Configure the following parameters:

Host Name

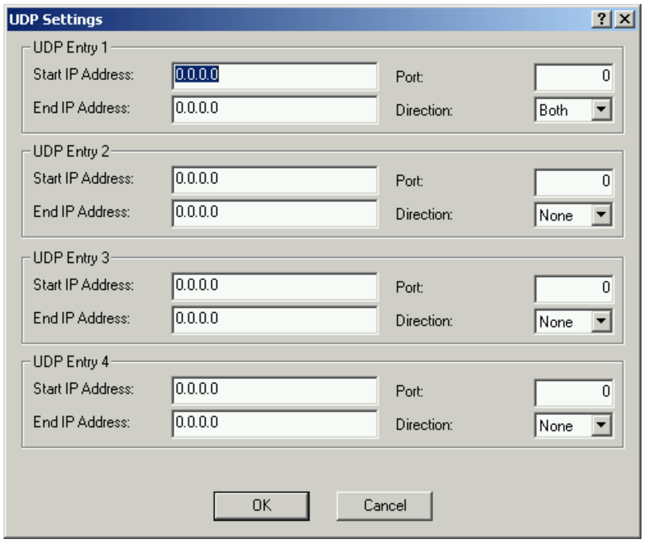
The name of the target host.

Port

The port number the target host is listening on for incoming connections.

UDP Settings

When the **Line Service** is set to **UDP**, the Device Server processes UDP packets according to the UDP settings.



UDP Entry 1
Start IP Address: 0.0.0.0 Port: 0
End IP Address: 0.0.0.0 Direction: Both

UDP Entry 2
Start IP Address: 0.0.0.0 Port: 0
End IP Address: 0.0.0.0 Direction: None

UDP Entry 3
Start IP Address: 0.0.0.0 Port: 0
End IP Address: 0.0.0.0 Direction: None

UDP Entry 4
Start IP Address: 0.0.0.0 Port: 0
End IP Address: 0.0.0.0 Direction: None

Configure the following parameters:

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

End IP Address The last host IP address in the range of IP addresses (for IPV4, not required for IPV6) that the Device Server will listen for messages from and/or send messages to.

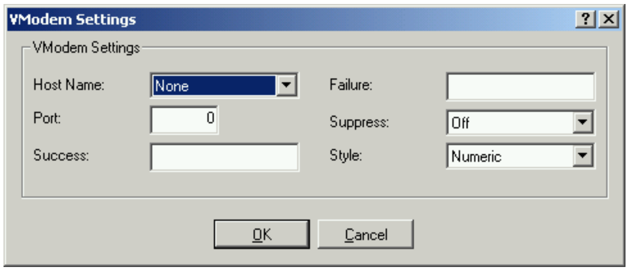
Port The port that the Device Server will use to receive messages from or relay messages to servers/hosts.

Direction The direction in which information is received or relayed:

- **None**—UDP service not enabled.
- **In**—LAN to serial.
- **Out**—Serial to LAN.
- **Both**—Messages are relayed both directions.

VModem Settings

When the **Line Service** is set to **VModem**, the Device Server acts as a virtual modem. After a virtual modem connection is established, data will flow in both directions in its original format.



Host Name: None
Port: 0
Success:
Failure:
Suppress: Off
Style: Numeric

Configure the following parameters:

Host Name The target host name.

Port The port number the target host is listening on for messages.

Success String that is sent to the serial device when a connection succeeds. If no string is entered, then the string `CONNECT` will be sent with the connecting speed, for example `CONNECT 9600`.

Failure String that is sent to the serial device when a connection fails. If no string is entered, then the string `NO CARRIER` will be sent.

Suppress If set to **No**, connection success/failure indication strings are sent to the connected device, otherwise these indications are suppressed.

Style One of the following:

- **Verbose**—Return codes (strings) are sent to the connected device.
- **Numeric**—The following characters can be sent to the connected device:

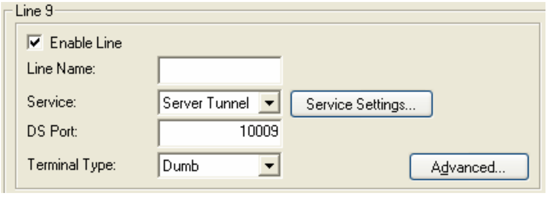
  1 Successfully Connected

  2 Failed to Connect

  4 Error

Server Tunnel Settings

The purpose of the serial **Line Service Client/Server Tunnel** is to allow two Device Servers that are connected back-to-back over Ethernet to virtually link two serial ports. The serial device that initiates the connection is the **Client Tunnel** and the recipient is the **Server Tunnel**, although once the communication tunnel has been successfully established, the communication tunnel will stay connected and can go both ways. The Server Tunnel will support Telnet Com Port Control protocol as detailed in RFC 2217. See ***Serial Tunnel Settings*** on page 43 for more information about how to configure the Device Server for a serial tunnelling.

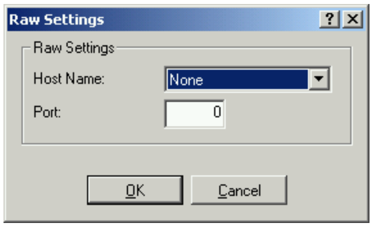


☑ Enable Line
Line Name:
Service: Server Tunnel
DS Port: 10009
Terminal Type: Dumb

It is important that the **Client Tunnel Port** parameter reflect the **DS Port** set for the Line when the Device Servers are being used back-to-back over Ethernet.

Client Tunnel Settings

The purpose of the serial **Line Service Client/Server Tunnel** is to allow two Device Servers that are connected back-to-back over Ethernet to virtually link two serial ports. The serial device that initiates the connection is the **Client Tunnel** and the recipient is the **Server Tunnel**, although once the communication tunnel has been successfully established, the communication tunnel will stay connected and can go both ways. See ***Serial Tunnel Settings*** on page 43 for more information about how to configure the Device Server for a serial tunnelling.



Raw Settings

Raw Settings

Host Name: None

Port: 0

Configure the following parameters:

Host Name

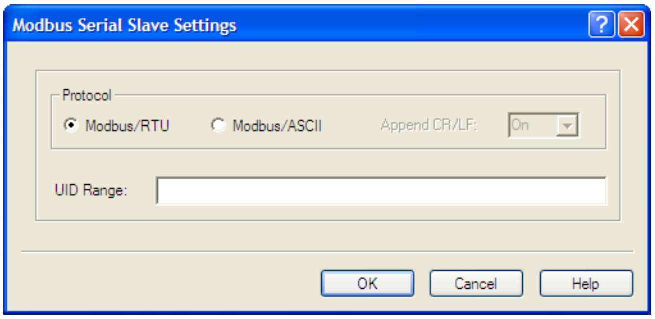
The name of the Device Server that is connected to the serial device, acting as the Server Tunnel.

Port

The **DS Port** of the Device Server that is connected to the serial device.

Modbus Slave Settings

This window configures the parameters for Modbus Slaves residing on the serial side of the Device Server. See ***Modbus Configuration*** on page 35 for more information about how to configure the Device Server for a Modbus environment.



Modbus Serial Slave Settings

Protocol

● Modbus/RTU ○ Modbus/ASCII Append CR/LF: On

UID Range:

Configure the following parameters:

Modbus/RTU

Select this option if the Modbus Master is configured using the Modbus/RTU protocol.

Modbus/ASCII

Select this option if the Modbus Master is configured using the Modbus/ASCII protocol.

Append CR/LF

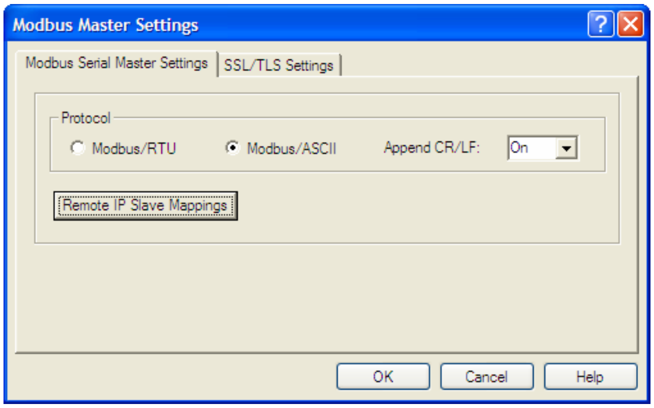
When **Modbus/ASCII** is selected, adds a CR/LF to the end of the transmission; most Modbus devices require this option. The default is **On**.

UID Range

You can specify a range of UIDs (1-247), in addition to individual UIDs. The format is comma delimited; for example, 2-35, 50, 100-103.

Modbus Master Settings

This window configures the parameters for Modbus Masters on the serial side of the Device Server. You can also choose to transmit the Modbus Master data encrypted via SSL/TLS. See ***Modbus Configuration* on page 35** for more information about how to configure the Device Server for a Modbus environment.



○ Modbus/RTU ● Modbus/ASCII Append CR/LF: On

Configure the following parameters:

Modbus/RTU

Select this option if the Modbus Slave is configured using the Modbus/RTU protocol.

Modbus/ASCII

Select this option if the Modbus Slave is configured using the Modbus/ASCII protocol.

Append CR/LF

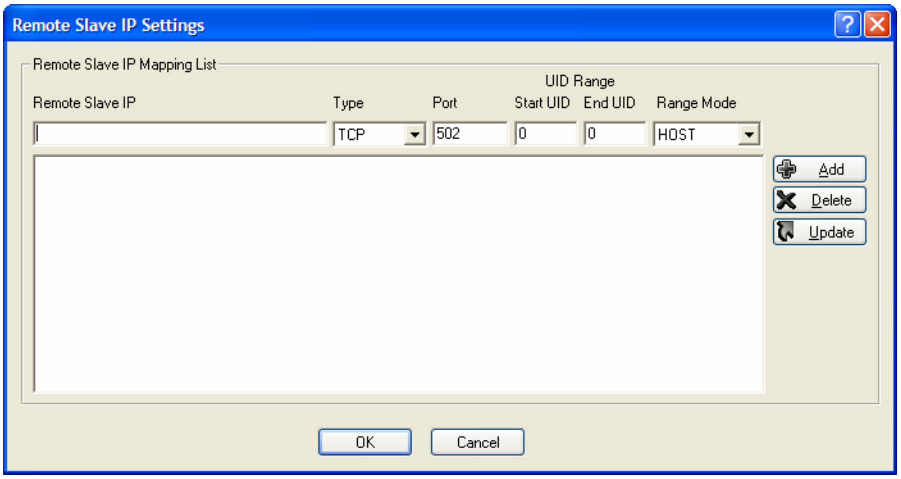
When **Modbus/ASCII** is selected, adds a CR/LF to the end of the transmission; most Modbus devices require this option. The default is **On**.

Remote IP Slave Mappings Button

Click this button to launch the Remote Slave IP Settings window, where you can configure the TCP/Ethernet Modbus Slaves that the Modbus Master on the Line will communicate with.

Remote IP Slave Mappings

This window allows you to configure all the Modbus Slaves, which reside on the Ethernet/TCP side of the Device Server, that will be receiving messages from the Modbus Master. See ***Modbus Configuration*** on page 35 for more information about how to configure the Device Server for a Modbus environment.



Type: TCP
Port: 502
Start UID: 0
End UID: 0
Range Mode: HOST

Configure the following parameters:

Remote Slave IP The IP address of the TCP/Ethernet Modbus Slave.

Protocol Specify the protocol that is used between the Modbus Master and Modbus Slave(s), either TCP or UDP.

Port The destination port of the remote Modbus TCP Slave that the Device Server will connect to.

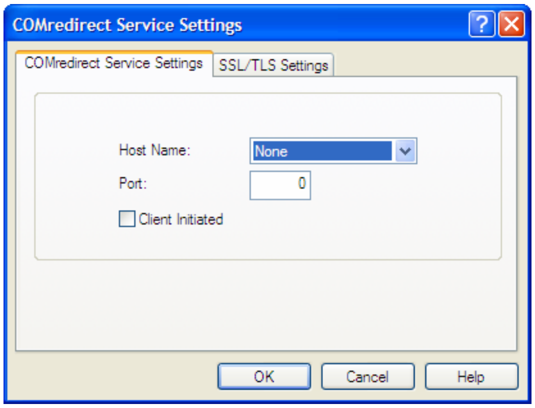
Start UID When **Range Mode** is **Host** and you have sequential Modbus Slave IP addresses (for example, 10.10.10.1, 10.10.10.2, 10.10.10.3, etc.), you can specify a UID range and the Device Server will automatically increment the last digit of the configured IP address. Therefore, you can specify a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

End UID When **Range Mode** is **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 Device Server will automatically increment the last digit of the configured IP address. Therefore, you can specify a UID range of 1-100, and the Device Server will route Master Modbus messages to all Modbus Slaves with IP addresses of 10.10.10.1 - 10.10.10.100.

Range Mode If you specify **Host**, the IP address is used for the first UID specified in the range. The last octect in the IPv4 address is then incremented for subsequent UID's in that range. The **Host** option is not applicable for IPv6 addresses. If you specify **Gateway**, the Modbus Master Gateway will use the same IP address when connecting to all the remote Modbus slaves in the specified UID range.

COMredirect Settings

When the **Line Service** is set to **COMredirect**, data is sent through the connection in its original format. This raw TCP/IP connection can be initiated from the Device Server to the configured host or from the host to the Device Server, depending on the settings.



Host Name: None

Port: 0

□ Client Initiated

Configure the following parameters:

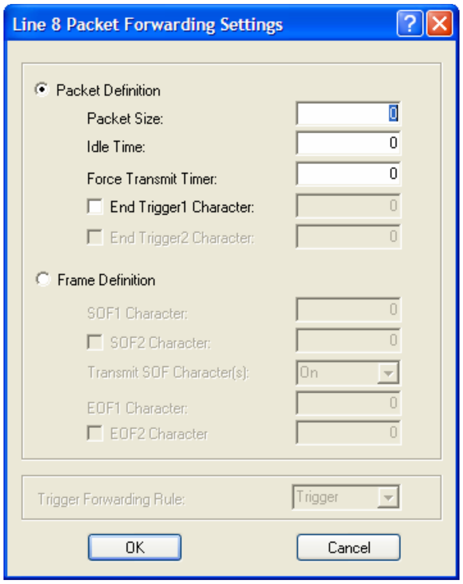
Host Name The name of the target host.

Port The port number the target host is listening on for incoming connections.

Client Initiated When enabled, allows the TruePort client to initiate communication to the Device Server.

Packet Forwarding

The Packet Forwarding feature allows you to control how the data coming from a serial device is packetized before forwarding the packet onto the LAN network.



Line 8 Packet Forwarding Settings

● Packet Definition

Packet Size: 0

Idle Time: 0

Force Transmit Timer: 0

□ End Trigger1 Character: 0

□ End Trigger2 Character: 0

○ Frame Definition

SOF1 Character: 0

□ SOF2 Character: 0

Transmit SOF Character(s): On

EOF1 Character: 0

□ EOF2 Character 0

Trigger Forwarding Rule: Trigger

Configure the following parameters:

Packet Definition

This section 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.

Packet Size

The number of byte that must be received from the serial port before the packet is transmitted to the network. A value of zero (0) ignores this parameter. Valid values are 0-1024 bytes. The default is 0.

Idle Time

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. Valid values are 0-65535 ms. The default is 0.

Force Transmit Timer

When the specified amount of time, in milliseconds, elapses after the first character is received from the serial port sender, the packet is transmitted. A value of zero (0) ignores this parameter. Valid values are 0-65535 ms. The default is 0.

End Trigger1 Character

When enabled, specifies the character that when received will define when the packet is ready for transmission. The actual transmission of the packet is based on the Trigger Forwarding Rule. Valid values are in hex 0-FF. The default is 0.

End Trigger2 Character

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 Device Server waits for another End Trigger1 character to start the End Trigger1/End Trigger2 character sequence). The actual transmission of the packet is based on the Trigger Forwarding Rule. Valid values are in hex 0-FF. The default is 0.

Frame Definition

This section 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. The default frame definition is SOF=00 and EOF=00.

SOF1 Character

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. Valid values are in hex 0-FF. The default is 0.

SOF2 Character

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 Device Server waits for another SOF1 character to start the SOF1/SOF2 character sequence). Valid values are in hex 0-FF. The default is 0.

Transmit SOF Character(s)

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.

EOF1 Character

Specifies the End of Frame character, which defines when the frame is ready to be transmitted. The actual transmission of the frame is based on the Trigger Forwarding Rule. Valid values are in hex 0-FF. The default is 0.

EOF2 Character

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 Device Server waits for another EOF1 character to start the EOF1/EOF2 character sequence), which defines when the frame is ready to be transmitted. The actual transmission of the frame is based on the Trigger Forwarding Rule. Valid values are in hex 0-FF. The default is 0.

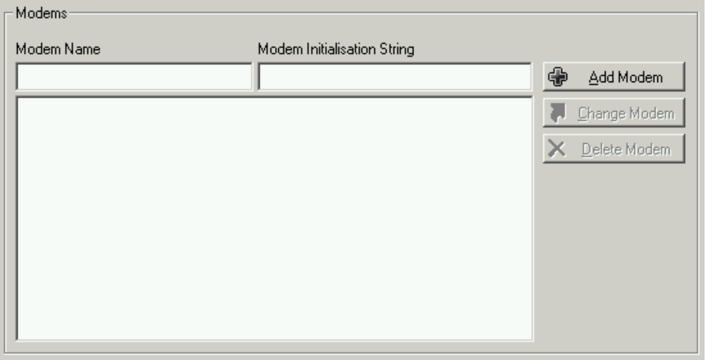
Trigger Forwarding Rule

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:

- **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.

Configuring Modems

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



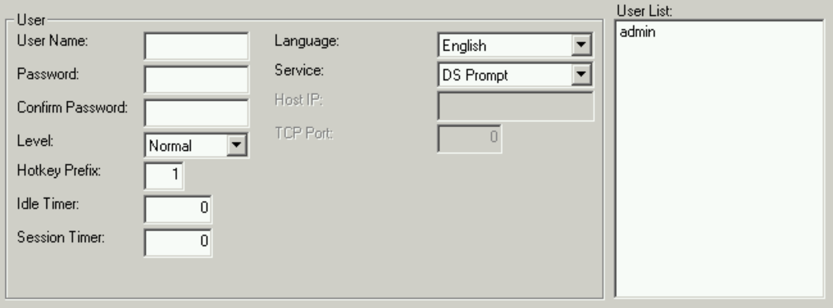
Configure the following parameters:

Modem Name The name of the modem. Do not use spaces.

Modem Initialisation String The initialisation string of the modem; see your modem’s documentation.

Configuring Users

You can configure up to four users in the Device Server’s local user database, in addition to the Admin user.



Configure the following parameters:

User Name The name of the user. Do not use spaces.

Password The password the user will need to enter to login to the Device Server.

Confirm Password Enter the user’s password again to verify it is entered correctly.

Level

The access that a user is allowed:

- **Admin**—The admin level user has total access to the Device Server. You can create more than one admin user account but we recommend that you only have one. They can monitor and configure the Device Server.
- **Normal**—The Normal level user has limited access to the Device Server. Limited CLI commands and Menu access are available with the ability to configure the user’s own configuration settings.
- **Restricted**—The Restricted level user can only access predefined sessions or access the Easy Port Access menu. Can only view or monitor the Device Server using CLI commands to display information about the Device Server.
- **Menu**—The menu level user will only be able to access predefined session or access the Easy Port Access menu. The Easy Port Access allows the user to connect to the accessible line without disconnecting their initial connection to the Device Server. Does not have any access to CLI commands.

Hotkey Prefix

The prefix that a user types to control the current session. The default value is **hex 01**, which corresponds to **Ctrl-a** (**^a**) (hex value 02 would be Ctrl-b (^b), etc.):

- **^a *number***—To switch from one session to another, press **^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 Device 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 Device Server. You will be returned to where you left off. The session will be left running.
- **^a l**—(Lowercase L) Locks the line until the user unlocks it. The user is prompted for a password (any password, excluding spaces) and locks the line. Next, the user must retype the password to unlock the line.
- **^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.

The **User Hotkey Prefix** value overrides the **Line Hotkey Prefix** value. You can use the **Hotkey Prefix** keys to lock a line only when the line **Lock** parameter is **On**.

Idle Timer

The amount of time, in seconds, that the **Idle Timer** will run. Use this timer to close a connection because of inactivity. When the **Idle Timer** expires, because there has been no exchange of data within the specified time, the Device Server will close the connection. The default value is **0** (zero), meaning that the **Idle Timer** will not expire (the connection is open permanently). The maximum value is 4294967 seconds. The **User Idle Timer** will override the **Line Idle Timer**, with the exception of reverse Telnet sessions.

Session Timer

The amount of time, in seconds, that the **Session Timer** will run. Use this timer to forcibly close a user’s session (connection). When the **Session Timer** expires, the Device Server will end the 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 maximum value is 4294967 seconds. The **User Session Timer** will override the **Line Session Timer**, with the exception of reverse Telnet sessions.

Language

You can specify whether a user will use **English** or **Customlang** as the language that appears in the Menu, CLI, or WebManager. The Device Server supports one custom language that must be downloaded to the Device Server; otherwise, **Customlang** defaults to English.

Service

The type of service that the user will use.

Host IP

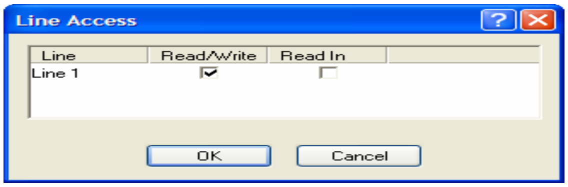
When the **User Service** is set to **Telnet** or **TCP_clear**, the target host IP address. If 255.255.255.255 is specified in the configuration, the user will be prompted for an IP address or hostname. If no IP address is specified, the Host IP value in the **Default User** configuration will be used. The default is **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.

Configuring Line Access

Line Access defines the read/write privileges that a user has while accessing a line.



Line	Read/Write	Read In
Line 1	☑	□

Configure the following options:

Line Access

Specifies the user access rights to each Device Server device line. Options are:

- **Read/Write**—Users are given read and write access to the line.
- **Read In**—Users are given access to read only outbound data, data that is going from the Device Server to the device.

Configuring Sessions

You can configure user **Sessions** to limit the access the user has to the network and the way the user connects to a host. Users who are **Level Normal** or **Admin** can define **Free Sessions**, in addition to using defined sessions. Users who are **Level Restricted** or **Menu** can only access predefined sessions.

Configure the following parameters:

Session

You can create up to four predefined sessions for each user. You can specify the connection service and its settings for each session.

Auto

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

The following **Session** connections are available:

- **None**—No connection is configured for this session.
- **Telnet**—For information on the Telnet configuration window, see ***Telnet Settings*** on page 64.

Configuring the Default User

When you add new users to the Device Server, they will initially inherit any parameters set in the **Default User** (the parameters can be changed on a per user basis).

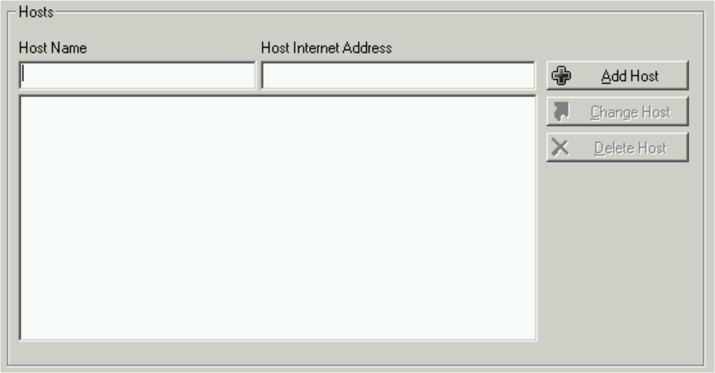
For information on the **Default User** configuration parameters, see ***Configuring Users*** on page 74.

Configuring the Network

The network configuration parameters define the network that the Device Server will be operating within.

Configuring Hosts

One of the first things you will probably want to configure is the hosts that the Device Server or Users will be interacting with, since most configuration windows require that the hosts already be configured. You can configure up to 20 hosts.

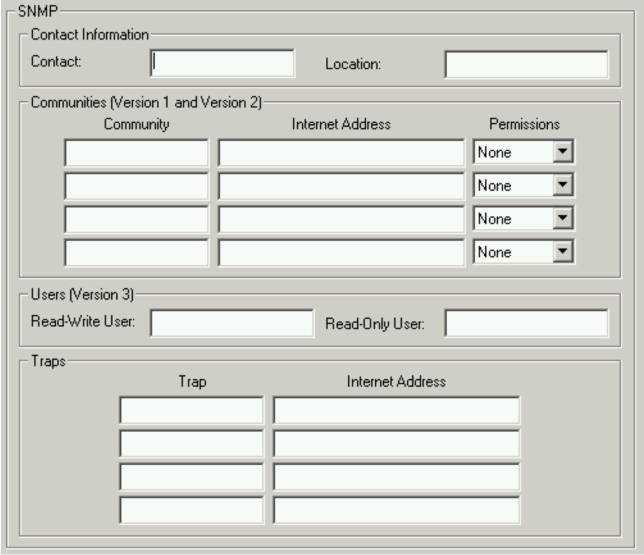


Configure the following parameters:

Host Name	The name of the host.
Host Internet Address	The host IP address.

Configuring SNMP

If you are using the Device Server SNMP MIB-based configuration/management option, you can use the DeviceManager to easily set up SNMP users, traps, and communities. The Device Server supports the SNMP traps for restart and SNMP community authentication error. For more information on SNMP, see ***SNMP*** on page 31.



Community	Internet Address	Permissions
		None
		None
		None
		None

Configure the appropriate parameters:

Contact

The name and contract information of the person who manages this SMNP node.

Location

The physical location of the SNMP node.

Community

A name that will be sent to the Device Server from an SNMP manager. This name will define the permissions of the manager.

Internet Address

The IP address of the SNMP manager that will send requests to the Device Server. If the address is **`0.0.0.0`**, any SNMP manager with the **Community Name** can access the Device Server.

Permissions

Permits the Device Server to respond to SNMP requests by:

- **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.

Read-Write User

Specified user can view and edit SNMP variables.

Read-Only User

Specified user can only view SNMP variables.

Trap

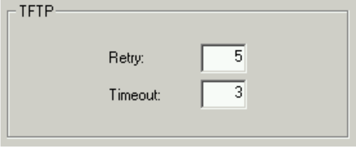
An arbitrary trap community name.

Internet Address

Defines the hosts (by IP address) that will receive trap messages generated by the Device Server. Up to four trap hosts can be defined.

Configuring TFTP

These parameters configure the TFTP settings for the Device Server's connections to hosts (as opposed to the TFTP settings under **Tools**, **Options**, which configure the TFTP settings for the DeviceManager's connection to a Device Server).



TFTP

Retry: 5

Timeout: 3

Configure the following parameters:

Retry

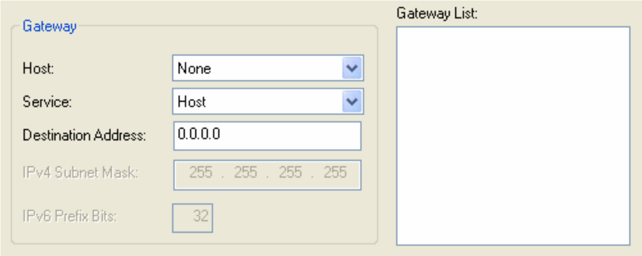
The number of times the Device Server will attempt to transfer (using TFTP) a file to/from a host. Enter a value between 0 and 5. The default is **5**. A value of **0** (zero) means that the Device Server will not attempt a retry should TFTP fail.

Timeout

The time, in seconds, that the Device Server will wait for a successful transmit or receipt of TFTP packets before retrying a TFTP transfer. Enter a value between 3 and 10. The default is **3** seconds.

Configuring Gateways

You can configure gateways to allow the Device Server access to hosts that are not within the local network segment.



Gateway

Host: None

Service: Host

Destination Address: 0.0.0.0

IPv4 Subnet Mask: 255 . 255 . 255 . 255

IPv6 Prefix Bits: 32

Gateway List:

Configure the following parameters:

Host

You can specify up to twenty hosts to act as gateways in your network. Each gateway host must be defined in the Device Server host table.

Service

Specify the type of gateway:

- **Default**—A gateway which provides general access beyond your local network.
- **Host**—A gateway reserved for accessing a specific host external to your local network.
- **Network**—A gateway reserved for accessing a specific network external to your local network.

Destination Address

When the gateway is a **Host** or **Network** gateway, you must specify the IP address of the target host machine/network.

IPv4 Subnet Mask

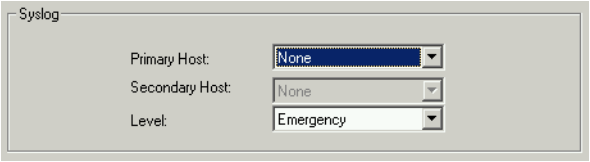
When the gateway is a **Network** gateway, you must specify the network's subnet mask.

IPv6 Prefix Bits

If the IP address is IPv6, then the Prefix Bits range is 0-128.

Configuring Syslog

You can configure where the system log messages are going to be sent and specify the lowest level message that the Device Server will send syslog messages for.



Syslog

Primary Host: None

Secondary Host: None

Level: Emergency

Configure the following options:

Primary Host

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

Secondary Host

If the Device Server cannot communicate with the primary host, then the Device Server will attempt to send system log messages to this preconfigured host; messages will be displayed on the host's monitor.

Level

Choose the event level that triggers a syslog entry:

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

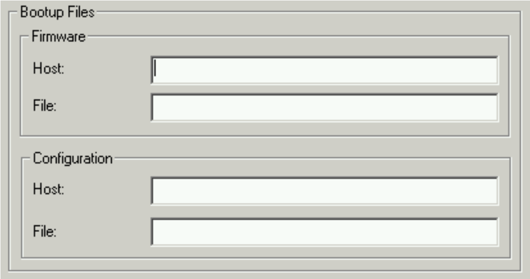
When you select a **Level**, all the levels that appear above it in the list also trigger a syslog entry. For example, if you select **Error**, all **Error**, **Critical**, **Alert**, and **Emergency** events will be logged.

Configuring Administration Tasks

You can specify new configuration and firmware files that will go into effect the next time the Device Server is rebooted and a message of the day (MOTD) file, whose contents will be displayed when User's log into the Device Server.

Configuring Bootup Files

When you specify a configuration and/or firmware file(s), the files will be downloaded via TFTP to the Device Server the next time it is rebooted.



Bootup Files

Firmware

Host:

File:

Configuration

Host:

File:

Configure the following parameters:

Firmware Host The host name or IP address of the server that contains the configuration or firmware file. If you use a host name, it must exist in the Device Server's host table or be resolved by DNS.

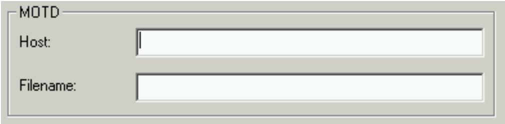
Firmware File The path and file name (do not use a drive letter), relative to the default path of your TFTP server software, of the update software for the Device Server that will be loaded when the Device Server is rebooted.

Configuration Host The host name or IP address of the server that contains the configuration or firmware file. If you use a host name, it must exist in the Device Server's host table or be resolved by DNS.

Configuration File The path and file name (do not use a drive letter), relative to the default path of your TFTP server software, of the configuration software for the Device Server that will be loaded when the Device Server is rebooted.

Configuring the MOTD File

You can specify a file whose content will be displayed to users after they connect to the Device Server, but before they log in. The Device Server will retrieve the file content every time a user connects to the Device Server, so you can change the content of the file without reconfiguring it within the Device Server.



Configure the following parameters:

Host	The host that the Device Server will be getting the Message of the Day file from.
Filename	The path and file name (do not use a drive letter), 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 Device Server.

Statistics

After you are connected to a Device Server, you can view statistics about the Device Server and its network environment. This can help you to troubleshoot problems or can provide valuable information about the Device Server's environment.

Tools

Saving a Configuration To File

When you connect to a Device Server, the Device Server's configuration is automatically uploaded to the DeviceManager. We suggest that you save the configuration to a file at this point, in case you need to revert to a working configuration in the future, by selecting **Tools**, **Save Configuration to File**. You can choose to save the configuration to the Device Server's native binary format or to a text file, which can be edited with a text editor. Either format can be reloaded into the DeviceManager at any time.

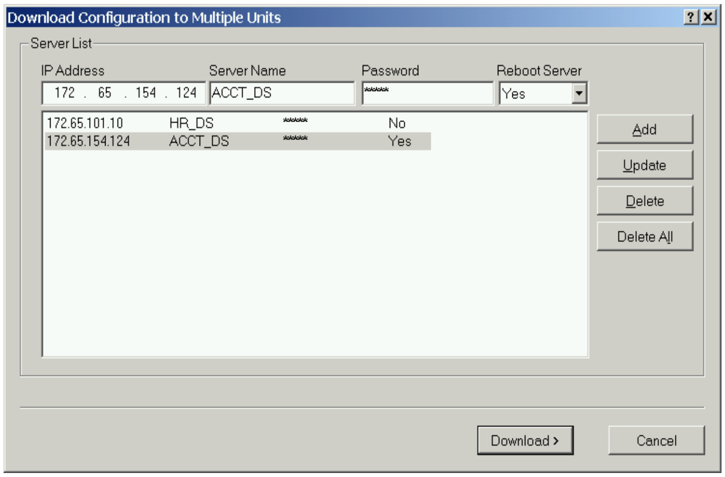
Getting a Configuration File

The DeviceManager can get a local configuration file (either binary or text) when you select **Tools**, **Get Configuration**, **Import from File**. The DeviceManager can also get the configuration from the Device Server it's connected to when you select **Tools**, **Get Configuration**, **Upload from Unit**; this can be useful if you've made changes to the Device Server's configuration that you would like to discard, you can simply reload the Device Server's current configuration into the DeviceManager.

Configuring Multiple Device Servers

You can configure multiple Device Servers at one time with the active configuration file. Any value in the configuration file's **Server Name** and **Internet Address** parameters will be overwritten by the values specified in the **Server Name** and **IP Address** fields (these fields cannot be left blank)

1. Select **Tools**, **Download Configuration to Multiple Units**. The Download Configuration to Multiple Units window is displayed.



IP Address: 172 . 65 . 154 . 124
Server Name: ACCT_DS
Password: *****
Reboot Server: Yes

172.65.101.10	HR_DS	*****	No
172.65.154.124	ACCT_DS	*****	Yes

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

IP Address Enter the IP address of the Device Server that you want to download the configuration to.

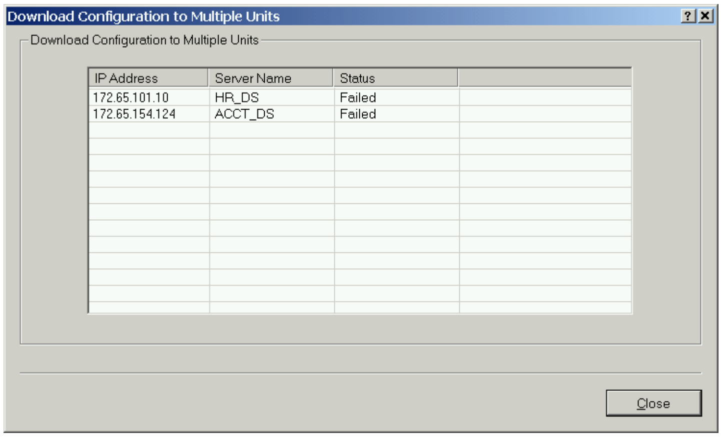
Server Name The name of the Device Server. The Device Server name that you put in this field is passed into the configuration before it is downloaded to the Device Server and cannot be left blank.

Password Enter the Admin user password for the Device Server.

Reboot Server Determines whether or not the Device Server is rebooted after it has received the new configuration. The new configuration definitions will not go into effect until the Device Server is rebooted.

3. Click **Add** to add the Device Server to the download list. You can also click on a Device 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.



Download Configuration to Multiple Units
? X
Download Configuration to Multiple Units
Close

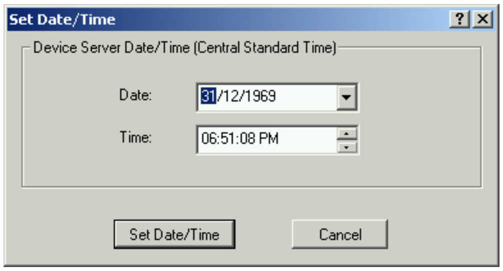
IP Address	Server Name	Status
172.65.101.10	HR_DS	Failed
172.65.154.124	ACCT_DS	Failed

Downloading Device Server Firmware

To upgrade the Device Server firmware (software), select **Tools**, **Download Firmware to Unit**. Once the firmware download is complete, you will be prompted to reboot the Device Server. You can choose to reboot the Device Server at another time by selecting **Tools**, **Reboot Server**. Upgrading the firmware does not affect the Device Server's configuration file or downloaded custom files.

Setting the Device Server's Date and Time

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



Date: 31/12/1969

Time: 06:51:08 PM

Configure the following parameters:

Date The Device Server's date. The format of the Device Server's date is dependent on the Windows operating system and regional settings.

Time The Device 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 Device Server's time zone is set to Eastern Standard Time (GMT -5:00), the Device Server's time is three hours ahead of your PC's time. If you set the Device Server's time to 2:30 pm, the Device Server's actual internal clock time is 5:30 pm.

Rebooting the Device Server

When you download any file (configuration, keys, certificates, firmware, etc.) to the Device Server, you must reboot the Device Server for it to take effect by selecting **Tools**, **Reboot Server**.

Resetting the Device Server to Factory Defaults

You can reset the Device Server to its factory default configuration by selecting **Tools**, **Reset to Factory Default**. The Device Server will automatically reboot itself with the factory default configuration.

Resetting a Line

After you make changes to the **Line** configuration parameters and click the **Apply** button, you can reset the line to test the changes by selecting **Tools**, **Kill Line**. If you are happy with the configuration changes, you can download the configuration by selecting **Tools**, **Download Configuration to Unit**. Of course, your new configuration will not take effect until you reboot the Device Server by selecting **Tools**, **Reboot Server**.

Custom Files

Saving Crashes to a Dump File

If the Device Server should crash, you can save the crash information (dump) to a file that can be sent to Technical Support for interpretation. This should probably be done only under the guidance of Technical Support.

Downloading Terminal Definitions

You can create up to three custom terminal definitions and download them to the Device Server (if you need a terminal definition that is not currently defined within the Device Server). It is important that you remember which Device Server Terminal Definition you download your custom terminal definition under.

For example, if you download a custom terminal definition as **Terminal Definition 2**, you must select **Terminal Type Term2** in the **Line** window to use that terminal definition.

See ***Creating Terminal Definition Files*** on page 47 for information on creating custom terminal definitions.

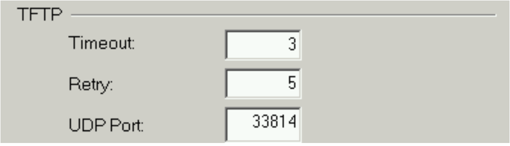
Downloading a Language File

You can download one custom language file that can be specified in the **User** configuration window. See ***Language Support*** on page 45 for information on creating custom language files.

Setting DeviceManager Options

When you select **Tools**, **Options**, you can set the following:

- **Confirmation Messages**—Specify whether you want to receive confirmation messages for all of the following selections:
    - **Tools**, **Download Configuration to Unit**
    - **Tools**, **Reboot Server**
    - **Tools**, **Reset to Factory Defaults**
    - **Tools**, **Reset SecurID Node Secret**
    - **Tools**, **Kill Line**
    - Anytime you click a **Delete** button
- **TFTP**—Sets the TFTP options for communication between the DeviceManager and a Device Server.



TFTP

Timeout: 3

Retry: 5

UDP Port: 33814

Configure the following parameters:

Retry

The number of times the DeviceManager will attempt to transfer (using TFTP) a file to/from a Device Server. Enter a value between 0 and 5. The default is **5**. A value of **0** (zero) means that the Device Server will not attempt a retry should TFTP fail.

Timeout

The time, in seconds, that the DeviceManager will wait for a successful transmit or receipt of TFTP packets before retrying a TFTP transfer. Enter a value between 3 and 10. The default is **3** seconds.

UDP Port

The port that the DeviceManager will use to TFTP to the Device Server. The default port is 33814 (ports 33812 and 33813 are also in use by the DeviceManager).

- **Statistics**—Specify whether or not you want to have the statistics automatically refresh and the refresh rate.

6 Command Line Interface

Introduction

This chapter provides the command line interface (CLI) options available for the Device Server. The commands are grouped by function.

CLI Conventions

This section explains how to interpret the CLI syntax.

Command Syntax

Each command is broken down into several categories:

- **Description**—Provides a brief explanation of how the command is used.
- **User Level**—Shows which user level(s) (Restricted, Normal, and/or Admin) can issue the command. Some commands have options that are available for one user level and not for another level; this usually occurs when a command is valid for both Normal and Admin user levels, where the Admin user level command will have extended options.
- **Syntax**—Shows the actual command line options. The options can be typed in any order on the command line. The syntax explanation will use the following command to break down the command syntax:

  ```
  set service [dhcp/bootp on|off] [telnetd on|off] [httpd on|off]
  [snmpd on|off] [spcd on|off] [syslog on|off] [dmgrd on|off]
  ```

  – Square brackets ([]) show the options that are available for the command. You can type a command with each option individually, or string options together in any order you want. For example,

  ```
  set service dhcp/bootp on telnetd off
  ```

  – Angle brackets (<>) show that the text inside the brackets is a description for a variable value that you must fill in according to your requirements. In the **`set server`** command, you must determine the values for **`domain`**, **`internet`**, **`name`**, **`password-limit`**, and **`subnet-bit-length`**, if you wish to specify them and not use their defaults (default values provided in the **Options** description). The angle brackets can also contain a range that can be used.

  – The pipe (|) shows an ’or’ condition. For example, valid values for **`telnetd`** are either **`on`** or **`off`**.
- **Options**—Provides an explanation of each of the options for a command and the default value if there is one. Some commands do not have any options, so this category is absent.

Command Shortcuts

When you type a command, you can specify the shortest unique version of that command or you can press the **ESC** or **TAB** key to complete the command. For example, the following command:

```
set telnet-client map-to-crlf off
```

can be typed as:

```
set tel map off
```

or, you can use the **ESC** key to complete the lines as you go along:

```
set tel<ESC>net-client ma<ESC>p-to-crlf off
```

where the <**ESC**> key was pressed to complete the option as it was typed.

Command Options

When you are typing commands on the command line (while connected to the Device Server), you can view the options by typing a question mark (**?**) after any part of the command to see what options are available/valid. For example:

```
DS$ set vmodem ?
failure-string
host
port
style
success-string
suppress
DS$ set vmodem failure-string ?
<text>                   30 characters maximum
DS$ set vmodem failure-string "Vmodem failed" ?
failure-string
host
port
style
success-string
suppress
Or press Enter to confirm command
DS$ set vmodem failure-string "Vmodem failed"
DS$ show vmodem
Host
Host Port
Success String
Failure String           "Vmodem failed"
Suppress                 Off
Style                    Numeric
DS$
```

Server Commands

This section defines all the CLI commands associated with configuring the Device Server's server parameters.

Server Commands

Set Server

Description Sets server parameters.

User Level Admin

Syntax

```
set server [banner on|off] [bypass-password on|off]
 [domain <string>] [flush-on-close on|off]
 [internet <IPV4_address>] [name <string>] [oem-login on|off]
 [password-limit <0-10>] [prompt-with-name on|off]
 [single-telnet on|off] [netmask <IPV4_address>]

set server tftp [retry <integer>] [timeout <integer>]
```

Options

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. The default is **Off**.

bypass-password

When set, authorised 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**.

domain_name

Unique name for your domain, your location in the global network. Like Hostname, it is a symbolic, rather than a numerical, identifier.

flush-on-close

When enabled, deletes any pending data when a port is closed; as opposed to maintaining the port to send pending data. The default value is **Off**.

internet

The Device Server's unique IPv4 network IP address. If you are using the Device Server in an IPv6 network, this field can be left blank.

oem-login

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:`.

password-limit

The number of attempts a user is allowed to enter a password for a port. If this limit is exceeded, the port is disabled for 5 minutes. A user with Admin level rights can restart the port, bypassing the timeout, by issuing a kill on the disabled port. The default value is **3**.

prompt-with-name

Displays the **Server Name** field value instead of default product name. When enabled, the **Server Name** is displayed in the Device Server login prompt, CLI prompt, WebManager login screen, and the heading of the Menu. The default value is **Off**.

single-telnet

Sets all reverse connections (raw and telnet) to a one connection at a time mode. Server-side applications will get a (socket) connection refused until:

- 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

This also enables a per-connection keepalive 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 recognised by the reverse service (all connections).

Applications using Single Telnet 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; this is to allow any data sent on prior connections to be transmitted out of the serial port. Application network retry logic needs to accommodate this feature. The default value is **Off**.

subnet-bit-length

The number of bits in the subnet mask. For example, a subnet mask of 255.255.0.0 has 16 subnet/prefix bits. Valid values are 0-31. The default is 0. When the value is 0, the correct value is determined based on the class of the **IP Address**.

retry

The number of times the Device Server will attempt to transfer (using TFTP) a file to/from a host. Enter a value between 0 and 5. The default is **5**. A value of **0** (zero) means that the Device Server will not attempt a retry should TFTP fail.

timeout

The time, in seconds, that the Device Server will wait for a successful transmit or receipt of TFTP packets before retrying a TFTP transfer. Enter a value between 3 and 10. The default is **3** seconds.

Set Service

Description Sets server service parameters.

User Level Admin

Syntax

```
set service [dhcp/bootp on|off] [telnetd on|off] [httpd on|off]
 [snmpd on|off] [spcd on|off] [syslog on|off] [dmgrd on|off]
 [modbusd on|off]
```

Options **dhcp/bootp**

DHCP/BOOTP client process in the Device Server.

telnetd

Telnet daemon process in the Device Server on port 23.

httpd

HTTP daemon process in the Device Server on port 80.

snmpd

SNMP daemon process in the Device Server on port 161.

spcd

SPC (COMredirect) daemon process in the Device Server on port 688.

syslog

Syslog client process in the Device Server.

dmgrd

DeviceManager daemon process in the Device Server. If you disable this service, you will not be able to connect to the Device Server with the DeviceManager application. DeviceManagerD listens on port 33812 and sends on port 33813.

modbusd

Modbus daemon process in the Device Server on port 502.

Show Modbus

Description Shows the Modbus settings for the gateway.
User Level Normal, Admin
Syntax `show modbus gateway`

Show Server

Description Shows the parameters set for the server.
User Level Admin, Normal
Syntax `show server`

Hardware Commands

Set Ethernet

Description Sets the serial line speed and duplex.
User Level Admin
Syntax

```
set ethernet speed-and-duplex
 auto|10-half|10-full|100-half|100-full
```

Options **auto|10-half|10-full|100-half|100-full**

Define the ethernet connection speed at one of the following:

- **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**

Show Hardware

Description Shows the hardware settings/information.
User Level Normal, Admin
Syntax `show hardware`

Modbus Commands

Set Modbus Gateway

Description Sets the authentication method for the Device Server.

User Level Admin

Syntax

```
set modbus gateway [addr-mode embedded|re-mapped]
  [broadcast on|off] [char-timeout <number>]
  [req-next-delay <number>] [exceptions on|off]
  [idle-timer <number>] [mess-timeout <number>]
  [port <TCP/UDP_port>] [req-queuing on|off]
  [remapped-id <1-247>] [ssl on|off]
```

Options

addr-mode

Determines if the original UID address will be embedded in the transmission header or if a specified (remapped) UID will be embedded in the transmission header.

broadcast

When enabled, a UID of 0 (zero) indicates that the message will be broadcast to all Modbus Slaves. The default is **Off**.

char-timeout

Used in conjunction with the Modbus RTU protocol, specifies how long to wait, in milliseconds, after a character to determine the end of frame. The default is **30** ms.

req-next-delay

A delay, in milliseconds, to allow serial slave(s) to re-enable receivers before issuing next Modbus Master request. The default is **50** ms.

exceptions

When enabled, an exception message is generated and sent to the initiating Modbus device when any of the following conditions are encountered: there is an invalid UID, the UID is not configured in the Gateway, there is no free network connection, there is an invalid message, or the target device is not answering the connection attempt. The default is **On**.

idle-timer

Specifies the number of seconds that must elapse without any network or serial traffic before a connection is dropped. If this parameter is set to 0 (zero), a connection will not be dropped (with the following exceptions: the TCP KeepAlive causes the connection to be dropped or the Modbus device drops the connection). The default is **10** seconds.

mess-timeout

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. The default is **1000** ms.

port

The network port number that the Slave Gateway will listen on for both TCP and UDP messages. The default is **502**.

req-queuing

When enabled, allows multiple, simultaneous messages to be queued and processed in order of reception. The default is **On**.

remapped-id

Specify the UID that will be inserted into the message header for the Slave Modbus serial device. Valid values are 1-247.

ssl

When enabled, Modbus Slave Gateway messages to remote TCP Modbus Masters are encrypted via SSL/TLS.

Show Modbus

Description Sets the authentication method for the Device Server.
User Level Admin
Syntax

```
show modbus gateway

show modbus slave|master <line_number>
```

COMredirect Baud Commands

Set COMredirect Remap-Baud

Description Sets the COMredirect baud remapping values.
User Level Admin
Syntax

```
set COMredirect remap-baud
 50|75|110|134|150|200|300|600|1200|1800|2400|4800|9600|19200|
   38400
 50|75|110|134|150|200|300|600|1200|1800|2400|4800|9600|19200|
   38400|57600|115200|230400|28800|[custom <baud_rate>]
```

Options **50|75|110|134|150|200|300|600|1200|1800|2400|4800|9600|19200|38400**

The configured baud rate of the COMredirect client.

50|75|110|134|150|200|300|600|1200|1800|2400|4800|9600|19200|38400|57600|115200|230400|28800|[custom <*baud_rate*>**]**

The actual baud rate that runs between the Device Server and the connected serial device. You can also specify a custom baud rate; valid values are 50-230400.

Show COMredirect

Description Shows the Device Server COMredirect remapping table.
User Level Normal, Admin
Syntax `show COMredirect`

User Commands

Logged Into the Device Server Commands

Admin

Description Changes a Normal-level user to the Admin user. When you press **Enter** after you type this command, you will be prompted for the Admin password.
User Level Normal
Syntax `admin`

Help

Description Displays help on using the command line interface (CLI).
User Level Restricted, Normal, Admin
Syntax `help`

Kill Line

Description Restarts a line.
User Level Normal, Admin
Syntax `kill line`

Kill Session

Description Kills an active session.
User Level Restricted, Normal, Admin
Syntax `kill session 1|2|3|4`

Options **1|2|3|4**

The number of the session(s) you want to kill.

Logout

Description Logs the user out from the Device Server.
User Level Restricted, Normal, Admin
Syntax `logout`

Menu

Description Switches from the CLI mode to the Menu.
User Level Restricted, Normal, Admin
Syntax `menu`

Ping

Description Pings the specified host/IP address.
User Level Normal, Admin
Syntax `ping <hostname/IP_address> [<packet_size>] [<#_of_packets>]`

Options <***hostname/IP_address***>

The name (host name or DNS name) or IP address of the machine you are trying to ping (verify the connection with).

<***packet_size***>

Enter the number of data bytes to be sent. The maximum size is 2000 bytes.

<***#_of_packets***>

Enter the number of the packets you want to send.

Resume

Description Resumes a started session.
User Level Restricted, Normal, Admin
Syntax `resume 1|2|3|4`

Options **1|2|3|4**

The number of the session you want to resume.

Screen

Description Switches from the CLI mode to the Menu.
User Level Restricted, Normal, Admin
Syntax `screen`

Set Termtype

Description Sets the type of terminal being used for the current session.
User Level Normal, Admin
Syntax

```
set termtype
 wyse60|vt100|ansi|dumb|tvi925|ibm3151te|vt320|hp700|term1|term2|
 term3
```

Option **wyse60|vt100|ansi|dumb|tvi925|ibm3151te|vt320|hp700|term1|term2|term3**

Specifies the type of terminal connected to the line:

- **Dumb**
- **WYSE60**
- **VT100**
- **ANSI**
- **TVI925**
- **IBM3151TE**
- **VT320** (specifically supporting VT320-7)
- **HP700** (specifically supporting HP700/44)
- **Term1, Term2, Term3 (user defined terminals)**

Set User

Description Sets the current user's settings.

User Level Normal, Admin

Syntax

```
set user . [hotkey-prefix <00-7f>] [language english|customlang]
 [password]
```

Options

hotkey-prefix

The prefix that a user types to control the current session. The default value is **hex 01**, which corresponds to **Ctrl-a** (**^a**) (hex value 02 would be Ctrl-b (^b), etc.):

- **^a *number***—To switch from one session to another, press **^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 Device 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 Device Server. You will be returned to where you left off. The session will be left running.
- **^a l**—(Lowercase L) Locks the line until the user unlocks it. The user is prompted for a password (any password, excluding spaces) and locks the line. Next, the user must retype the password to unlock the line.
- **^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.

The **User Hotkey Prefix** value overrides the **Line Hotkey Prefix** value. You can use the **Hotkey Prefix** keys to lock a line only when the line **Lock** parameter is **On**.

language

You can specify whether a user will use **English** or **Customlang** as the language that appears in the Menu, CLI, or WebManager. The Device Server supports one custom language that must be downloaded to the Device Server; otherwise, **Customlang** defaults to English.

password

The password the user will need to enter to login to the Device Server.

Set User Session

Description Sets the current user's session settings.

User Level Normal, Admin

Syntax

```
set user . session 1|2|3|4|* [auto on|off] [type off|telnet]

set user . session 1|2|3|4|* telnet-options [host <config_host>]
 [port <TCP_port>] [termtype <terminal_name>] [line-mode on|off]
 [map-cr-crlf on|off] [local-echo on|off] [echo <00-7f>]
 [eof <00-7f>] [erase <00-7f>] [intr <00-7f>] [quit <00-7f>]
```

Options

session

Specifies the session number (or all, *) that you are configuring.

auto

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

telnet-options

See ***Set Telnet-Client*** on page 111.

Show Line Users

Description Shows the users who are on the line.
User Level Admin
Syntax `show line users`

Syslog Console

Description Starts/stops or displays the status of the syslog console.
User Level Admin
Syntax

```
syslog console start|stop

syslog console status
```

Options

start|stop

Start or stop console logging. When console logging is enabled, syslog messages will be echoed to the current console. These messages are filtered based on the level set in the (remote) syslog options.

status

Displays the current console logging status (enabled or disabled).

Show Sessions

Description Shows available sessions.
User Level Restricted, Normal, Admin
Syntax `show sessions`

Show Termtype

Description Shows the terminal type for the current session.
User Level Admin
Syntax `show termtype`

Start

Description Starts a predefined session. Only inactive sessions are displayed.
User Level Restricted, Normal, Admin
Syntax `start 1|2|3|4`

Options

1|2|3|4

The number of the session that you want to start.

Telnet

Description Starts a telnet session to the specified host/IP address.
User Level Normal, Admin
Syntax

```
telnet <hostname/IP_address> [<tcp_port>]
 [termtype <terminal_name>] [line-mode on|off]
 [map-cr-crlf on|off] [local-echo on|off]
 [echo <00-7f>] [eof <00-7f>] [erase <00-7f>] [intr <00-7f>]
 [quit <00-7f>] [escape <00-7f>]
```

Options

<hostname/IP_address>

The name of the target host.

<tcp_port>

The port number the target host is listening on for incoming connections.

termtype

Type of terminal attached to this line; for example, ANSI or WYSE60.

line-mode

When **On**, keyboard input is not sent to the remote host until **Enter** is pressed, otherwise input is sent every time a key is pressed. Default is **Off**.

map-cr-crlf

Maps carriage returns (CR) to carriage return line feed (CRLF). The default value is **Off**.

local-echo

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 only be used when **Line Mode** is **On**. Default is **Off**.

echo

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 with a default value of **5** (ASCII value **^E**).

eof

Defines the end-of-file character. When Line Mode is On, entering the eof character as the first character on a line sends the character to the remote host. This value is in hexadecimal with a default value of **4** (ASCII value **^D**).

erase

Defines the erase character. When Line Mode is Off, typing the erase character erases one character. This value is in hexadecimal with a default value of **8** (ASCII value **^H**).

intr

Defines the interrupt character. Typing the interrupt character interrupts the current process. This value is in hexadecimal with a default value of **3** (ASCII value **^C**).

quit

Defines the quit character. Typing the quit character closes and exits the current telnet session. This value is in hexadecimal with a default value of **1c** (ASCII value **FS**).

escape

Defines the escape character. Returns you to the command line mode. This value is in hexadecimal with a default value of **1d** (ASCII value **GS**).

Version

Description Displays firmware version and build.
User Level Normal, Admin
Syntax `version`

Configuring Users

Add User

Description Adds a user. You can add and configure up to four users in the Device Server.
User Level Admin
Syntax **`add user <`*`username`*`>`**

Option <***username***>

The name of the user, without spaces. When you finish the command and press Enter, you will be prompted to enter and re-enter a password for the user.

Delete User

Description Deletes a user.
User Level Admin
Syntax

```
delete user <config_user>
```

Option *<config_user>*

You can see a list of users that can be deleted by typing **`delete user ?`**.

Set Default User

Description Configures the Default User.
User Level Admin
Syntax

```
set default user [hotkey-prefix <00-7f>]
 [idle-timer <0-4294967>] [ip-host <ip_address>]
 [language english|customlang]
 [level admin|normal|restricted|menu]
 [line-access readin|readwrite on|off]
 [service dsprompt|telnet|tcp-clear] [sess-timer <0-4294967>]
 [port tcp-clear|telnet <tcp_port>]
```

Options **hotkey-prefix**

The prefix that a user types to control the current session. The default value is **hex 01**, which corresponds to **Ctrl-a** (**^a**) (hex value 02 would be Ctrl-b (^b), etc.):

- **^a *number***—To switch from one session to another, press **^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 Device 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 Device Server. You will be returned to where you left off. The session will be left running.
- **^a l**—(Lowercase L) Locks the line until the user unlocks it. The user is prompted for a password (any password, excluding spaces) and locks the line. Next, the user must retype the password to unlock the line.
- **^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.

The **User Hotkey Prefix** value overrides the **Line Hotkey Prefix** value. You can use the **Hotkey Prefix** keys to lock a line only when the line **Lock** parameter is **On**.

idle-timer

The amount of time, in seconds, that the **Idle Timer** will run. Use this timer to close a connection because of inactivity. When the **Idle Timer** expires, because there has been no exchange of data within the specified time, the Device Server will close the connection. The default value is **0** (zero), meaning that the **Idle Timer** will not expire (the connection is open permanently). The maximum value is 4294967 seconds. The **User Idle Timer** will override the **Line Idle Timer**, with the exception of reverse Telnet sessions.

ip-host

When the **User Service** is set to **Telnet** or **TCP_clear**, the target host IP address. If 255.255.255.255 is specified in the configuration, the user will be prompted for an IP address or hostname. If no IP address is specified, the Host IP value in the **Default User** configuration will be used. The default is **0.0.0.0**.

language

You can specify whether a user will use **English** or **Customlang** as the language that appears in the Menu, CLI, or WebManager. The Device Server supports one custom language that must be downloaded to the Device Server; otherwise, **Customlang** defaults to English.

level

The access that a user is allowed:

- **Admin**—The admin level user has total access to the Device Server. You can create more than one admin user account but we recommend that you only have one. They can monitor and configure the Device Server.
- **Normal**—The Normal level user has limited access to the Device Server. Limited CLI commands and Menu access are available with the ability to configure the user's own configuration settings.
- **Restricted—**The Restricted level user can only access predefined sessions or access the Easy Port Access menu. Can only view or monitor the Device Server using CLI commands to display information about the Device Server.
- **Menu—**The menu level user will only be able to access predefined session or access the Easy Port Access menu. The Easy Port Access allows the user to connect to the accessible line without disconnecting their initial connection to the Device Server. Does not have any access to CLI commands.

password

The password the user will need to enter to login to the Device Server.

line-access

Specifies the user access rights to each Device Server device line. Options are:

- **Read/Write—**Users are given read and write access to the line.
- **Read In—**Users are given access to read only outbound data, data that is going from the Device Server to the device.

phone-number

The phone number the Device Server will dial to callback the user (you must have set **Callback** to **On**). Enter the number without spaces. To change the phone number, overwrite the previous entry; to clear the phone number, set it to **""** (double quotes without a space).

service

The type of service that the user will use.

sess-timer

The amount of time, in seconds, that the **Session Timer** will run. Use this timer to forcibly close a user's session (connection). When the **Session Timer** expires, the Device Server will end the 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 maximum value is 4294967 seconds. The **User Session Timer** will override the **Line Session Timer**, with the exception of reverse Telnet sessions.

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.

Set User

Description Sets user’s settings. Normal-level users can configure only their own settings. Admin-level users can configure any user’s settings, including their own (with the exception of their User Level, which must stay at Admin).

User Level Normal, Admin

Syntax

```
set user . [hotkey-prefix <00-7f>] [language english|customlang]
 [password]
```

Admin

```
set user .|<username>|* [hotkey-prefix <00-7f>]
 [idle-timer <0-4294967>] [ip-host <ip_address>]
 [language english|customlang]
 [level admin|normal|restricted|menu] [password]
 [line-access readin|readout|readwrite on|off]
 [service dsprompt|telnet|tcp-clear] [sess-timer <0-4294967>]
 [port tcp-clear|telnet <tcp_port>]
```

Options

hotkey-prefix

The prefix that a user types to control the current session. The default value is **hex 01**, which corresponds to **Ctrl-a** (**^a**) (hex value 02 would be Ctrl-b (^b), etc.):

- **^a *number***—To switch from one session to another, press **^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 Device 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 Device Server. You will be returned to where you left off. The session will be left running.
- **^a l**—(Lowercase L) Locks the line until the user unlocks it. The user is prompted for a password (any password, excluding spaces) and locks the line. Next, the user must retype the password to unlock the line.
- **^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.

The **User Hotkey Prefix** value overrides the **Line Hotkey Prefix** value. You can use the **Hotkey Prefix** keys to lock a line only when the line **Lock** parameter is **On**.

idle-timer

The amount of time, in seconds, that the **Idle Timer** will run. Use this timer to close a connection because of inactivity. When the **Idle Timer** expires, because there has been no exchange of data within the specified time, the Device Server will close the connection. The default value is **0** (zero), meaning that the **Idle Timer** will not expire (the connection is open permanently). The maximum value is 4294967 seconds. The **User Idle Timer** will override the **Line Idle Timer**, with the exception of reverse Telnet sessions.

ip-host

When the **User Service** is set to **Telnet** or **TCP_clear**, the target host IP address. If 255.255.255.255 is specified in the configuration, the user will be prompted for an IP address or hostname. If no IP address is specified, the Host IP value in the **Default User** configuration will be used. The default is **0.0.0.0**.

language

You can specify whether a user will use **English** or **Customlang** as the language that appears in the Menu, CLI, or WebManager. The Device Server supports one custom language that must be downloaded to the Device Server; otherwise, **Customlang** defaults to English.

level

The access that a user is allowed:

- **Admin—**The admin level user has total access to the Device Server. You can create more than one admin user account but we recommend that you only have one. They can monitor and configure the Device Server.
- **Normal**—The Normal level user has limited access to the Device Server. Limited CLI commands and Menu access are available with the ability to configure the user's own configuration settings.
- **Restricted**—The Restricted level user can only access predefined sessions or access the Easy Port Access menu. Can only view or monitor the Device Server using CLI commands to display information about the Device Server.
- **Menu—**The menu level user will only be able to access predefined session or access the Easy Port Access menu. The Easy Port Access allows the user to connect to the accessible line without disconnecting their initial connection to the Device Server. Does not have any access to CLI commands.

password

The password the user will need to enter to login to the Device Server.

line-access

Specifies the user access rights to each Device Server device line. Options are:

- **Read/Write—**Users are given read and write access to the line.
- **Read In**—Users are given access to read only outbound data, data that is going from the Device Server to the device.

service

The type of service that the user will use.

sess-timer

The amount of time, in seconds, that the **Session Timer** will run. Use this timer to forcibly close a user's session (connection). When the **Session Timer** expires, the Device Server will end the 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 maximum value is 4294967 seconds. The **User Session Timer** will override the **Line Session Timer**, with the exception of reverse Telnet sessions.

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.

Set User Session

Description Configures a user's session settings. See ***Set User Session*** on page 96 for the options descriptions.

User Level Admin

Syntax

```
set user .|<username> session 1|2|3|4|* [auto on|off]
 [type off|telnet]

set user .|<username> session 1|2|3|4|* telnet-options
 [host <config_host>] [port <TCP_port>]
 [termtype <terminal_name>] [line-mode on|off]
 [map-cr-crlf on|off] [local-echo on|off]
 [echo <00-7f>] [eof <00-7f>] [erase <00-7f>] [intr <00-7f>]
 [quit <00-7f>]
```

Show Default User

Description Shows the Default User's settings.

User Level Admin

Syntax `show default user`

Show User

Description Shows user configuration settings.

User Level Admin

Syntax `show user <configured_user>|.`

Options ***<configured_user>***

Show the settings for the specified user.

`.`

Show the settings for the current user.

Line Commands

Line Commands

Set Line

Description Configures line parameters.

User Level Normal, Admin

Syntax

```
set line [data-bits 5|6|7|8] [dial none|in|out|both]
 [idle-timer <0-4294967>] [line-name <name>]
 [modem-name <config_modem>] [pages 1|2|3|4|5|6|7]
 [parity none|even|odd|mark|space] [phone-number <phone_number>]
 [rev-sess-security on|off] [sess-timer <0-4294967>]
 [stop-bits 1|2|1.5] [termtype wyse60|vt100|ansi|dumb|tvi925|
   ibm3151te|vt320|hp700|term1|term2|term3]
```

Admin

```
set line ... [break on|off] [flowin on|off] [flowout on|off]
 [hotkey-prefix <00-7f>] [initial cli|menu] [keepalive on|off]
 [lock on|off] [motd on|off] [reset on|off]
 [dial-timeout <number>] [dial-retries <number>]
 [single-character on|off] [user <name>] [nouser]
```

Options

data-bits

Specifies the number of bits in a byte. The default is **8**.

dial

Determines how a modem will work on the line. If your user is remote and will be dialing in via modem or ISDN TA, set this parameter to **In**; if the Device Server is being used as a router, set this parameter to either **In**, **Out**, or **Both**, depending on which end of the link your Device Server is situated and how you want to initiate the communication.

idle-timer

Enter a time period, in seconds, for which the **Idle Timer** will run. Use this timer to close a connection because of inactivity. When the **Idle Timer** expires, the Device Server will end the connection. The maximum value is 4294967 seconds (about 49 days). The default value of **0** (zero) means the **Idle Timer** will not expire, so the connection is permanently open.

line-name

Provide a name for the line so it can be easily identified.

modem-name

The name of the predefined modem that is used on this line.

pages

For **DSLogin** line service, this is the number of video pages the terminal supports. Valid values are 1-7. The default is **5** pages.

parity

Specifies if you are using **Even**, **Odd**, or **No parity** on the line. If you want to force a parity type, you can specify **Mark** for 1or **Space** for 0.

phone-number

The phone number to use when **Dial** is set to **Out**.

rev-sess-security

Enables/disables login/password authentication, locally or externally, on reverse Telnet connections. The default is **Off**.

sess-time

Enter a time, in seconds, for which the **Session Timer** will run. Use this timer to forcibly close the session (connection). When the **Session Timer** expires, the Device Server will end the connection. The default value is **0** seconds so the port will never timeout. The maximum value is 4294967 seconds (about 49 days).

break

Specifies how a break is interpreted:

- **None**—The Device Server ignores the break key completely and it is not passed through to the host. This is the default setting.
- **Local**—The Device 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 Device Server translates this into a telnet break signal which it sends to the host machine.
- **Brkintr**—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).

flowin

Determines if input flow control is to be used. Default is **On**. This is active only when **Line Flow Control** is set to **Soft**, **Hard**, or **Both**.

flowout

Determines if output flow control is to be used. Default is **On**. This is active only when **Line Flow Control** is set to **Soft**, **Hard**, or **Both**.

hotkey-prefix

The prefix that a user types to lock a line or redraw the Menu. The default value is **hex 01**, which corresponds to **Ctrl-a** (**^a**) (hex value 02 would be Ctrl-b (^b), etc.):

- **^a l**—(Lowercase L) Locks the line until the user unlocks it. The user is prompted for a password (any password, excluding spaces) and locks the line. Next, the user must retype the password to unlock the line.
- **^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.

You can use the **Hotkey Prefix** key to lock a line only when the **Line Lock** parameter is **On**.

initial

Specifies the initial interface a user navigates when logging into the line; either the **Menu** or a prompt for the **CLI**. The default is **CLI**.

keepalive

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, either ensuring the connection stays active OR causing a dropped connection condition to be recognised by the reverse raw service.

Applications using this feature need to be aware that there might be some considerable delay between a network disconnection and the port being available for the next connection attempt; this is to allow any data sent on prior connections to be transmitted out of the serial port buffer. Application network retry logic needs to accommodate this feature.

lock

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

motd

Enables/disables the message of the day on the line.

user

For **DSLogin** line service, makes this a line that is dedicated to the specified user. Only this user will be able to log in on this line and they won’t need to enter their login name - just their password.

nouser

Blanks out the User parameter, in case you want to change a dedicated user line to an undedicated line.

reset

Resets the terminal type connected to the line when a user logs out.

dial-timeout

The number of seconds the Device Server will wait to establish a connection to a remote modem. The default value is **45** seconds.

dial-retries

The number of times the Device Server will attempt to establish a connection with a remote modem. The default value is **2**.

single-character

When enabled, causes the Device Server to process every character as it comes in, as opposed to buffering the characters before processing; this provides better latency at the expense of efficiency.

stop-bits

Specifies the number of stop bits that follow a byte.

term-type

Specifies the type of terminal connected to the line:

- **Dumb**
- **WYSE60**
- **VT100**
- **ANSI**
- **TVI925**
- **IBM3151TE**
- **VT320** (specifically supporting VT320-7)
- **HP700** (specifically supporting HP700/44)
- **Term1, Term2, Term3 (user defined terminals)**

Set Line Interface

Description Configures line interface (hardware) parameters.

User Level Admin

Syntax

```
set line interface eia-232 [monitor-dcd on|off]
 [monitor-dsr on|off] [flow none|soft|hard|both]
 [speed 50|75|110|134|150|200|300|600|1200|1800|2400|4800|9600|
   19200|38400|57600|115200|230400|28800|custom <baud_rate>]

set line interface eia-422 [flow none|soft|hard|both]
 [speed 50|75|110|134|150|200|300|600|1200|1800|2400|4800|
   9600|19200|38400|57600|115200|230400|28800|
   custom <baud_rate>]

set line interface eia-485-half-duplex
 [tx-driver-control auto|rts] [flow none|soft]
 [echo-suppression on|off]]
 [speed 50|75|110|134|150|200|300|600|1200|1800|2400|4800|
   9600|19200|38400|57600|115200|230400|28800|
    custom <baud_rate>]

set line interface eia-485-full-duplex
 [tx-driver-control auto|rts] [flow none|soft]
 [speed 50|75|110|134|150|200|300|600|1200|1800|2400|4800|
   9600|19200|38400|57600|115200|230400|28800|
   custom <baud_rate>]
```

Options **eia-232 | eia422 | 485**

Specifies the type of line that is being used with the Device Server. Select either **EIA-232**, **EIA-422**, or **EIA-485**.

monitor-dcd

Specifies whether the RS-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 Device Server detects a DCD signal, the line service is started. Default is **Off**. If both **Monitor DCD** and **Monitor DSR** are enabled, both signals must be detected before the line service is started.

monitor-dsr

Specifies whether the RS-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 Device Server detects a DSR signal, the line service is started. Default is **Off**. If both **Monitor DCD** and **Monitor DSR** are enabled, both signals must be detected before the line service is started.

flow

Defines whether the data flow is handled by the software (**Soft**), hardware (**Hard**), **Both**, or **None**.

tx-driver-control

Used with a **EIA-485** serial interface, if your application supports **RTS** (Request To Send), select this option. Otherwise, select **Auto**. Default is **Auto**.

duplex

Specify whether the line is **Full Duplex** (communication both ways at the same time) or **Half Duplex** (communication in one direction at a time).

echo-suppression

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 **On**. The default is echo suppression **Off**.

speed

Specifies the baud rate of the line; keep in mind that speed is affected by the length of the cable. You can also specify a custom baud rate; valid values are 50-230400.

Set Line Service

Description Sets the service for the line. For services that need further configuration, see ***Line Service Commands*** on page 111 to find the Line Service that you want to configure.

User Level Admin

Syntax

```
set line service bidir <config_host> <server_port> <host_port>

set line service direct|silent raw <config_host> <host_port>

set line service direct|silent telnet <config_host> [<host_port>]

set line service reverse raw|telnet <server_port>

set line service client-tunnel <config_host> <host_port>

set line service server-tunnel <server_port>

set line service dslogin|udp|vmodem|modbus-master|modbus-slave

set line service comredirect client-initiated off <config_host>
 <host_port>

set line service comredirect client-initiated on <server_port>
```

Options **bidir**

Allows a bidirectional connection on a port.

<config_host>

The name of the target host.

<server_port>

The Device Server port number.

<host_port>

The port number the target host is listening on for incoming connections.

direct

Direct connections bypass the Device Server, enabling the user to log straight into a specific host. A direct connection is recommended where a user logging in to the Device Server is not required. It is also recommended where multiple sessions are not a requirement. The message **`Press return to continue`** is displayed on the user's screen. The user must press a key to display the host login prompt. The message is redisplayed on logout.

silent

Silent connections are the same as direct connections, except they are permanently established. The host login prompt is displayed on the screen. Logging out redisplays 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.

raw

Creates a connection where no authentication takes place and data is passed unchanged.

telnet

Sets the line for a telnet connection.

reverse

Enables a TCP/IP host to establish a login connection on an external machine attached to a port. For example, to access machines like protocol converters, statistical multiplexors, or machines like routers, firewalls, servers, etc.

client-tunnel

Sets the line for a client tunnel connection.

server-tunnel

Sets the line for a server tunnel connection.

dslogin

The default connection. The Device Server displays a login on that line. For example, **DSLogin** is used when a System Administrator configures the Device Server or users starts a session(s) from the Device Server to hosts.

udp

Sets the line to listen for and/or send UDP data.

vmodem

The Device Server port behaves as if it were a modem to the attached device.

modbus-slave

Sets the line to act as a Modbus master.

modbus-master

Sets the line to act as a Modbus slave.

comredirect

Sets the line to communicate with the COMredirect utility. You must install the COMredirect utility on the host machine.

client-initiated

When this option is turned on, the Device Server will wait for a connection from the COMredirect host (see the COMredirect documentation for information on how to set up this feature on the COMredirect host). When this option is turned off, the Device Server will initiate the connection to the COMredirect host. The default is off.

Set Termtype

Description Sets the terminal type for the current terminal session. term1, term2, and term3 refer to the user-uploadable custom terminal definitions. If these are not present, the default is wyse60.

User Level Restricted, Normal, Admin

Syntax

```
set termtype
 [wyse60|vt100|ansi|dumb|tvi925|ibm3151te|vt320|hp700|term1|term2
 |term3]
```

Option **wyse60|vt100|ansi|dumb|tvi925|ibm3151te|vt320|hp700|term1|term2|term3**

Specifies the type of terminal connected to the line:

- **Dumb**
- **WYSE60**
- **VT100**
- **ANSI**
- **TVI925**
- **IBM3151TE**
- **VT320** (specifically supporting VT320-7)
- **HP700** (specifically supporting HP700/44)
- **Term1, Term2, Term3 (user defined terminals)**

Show Line

Description Shows the line settings/information.

User Level Admin

Syntax `show line`

Line Service Commands

Set Telnet-Client

Description Configures telnet parameters.

User Level Normal, Admin

Syntax

```
set telnet-client [termtype <terminal_name>] [line-mode on|off]
 [map-cr-crlf on|off] [local-echo on|off] [echo <00-7f>]
 [eof <00-7f>] [erase <00-7f>] [intr <00-7f>] [quit <00-7f>]
 [escape <00-7f]
```

Options

termtype

Type of terminal attached to this line; for example, ANSI or WYSE60.

line-mode

When **On**, keyboard input is not sent to the remote host until **Enter** is pressed, otherwise input is sent every time a key is pressed. Default is **Off**.

map-cr-crlf

Maps carriage returns (CR) to carriage return line feed (CRLF). The default value is **Off**.

local-echo

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 only be used when **Line Mode** is **On**. Default is **Off**.

echo

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 with a default value of **5** (ASCII value **^E**).

eof

Defines the end-of-file character. When Line Mode is On, entering the eof character as the first character on a line sends the character to the remote host. This value is in hexadecimal with a default value of **4** (ASCII value **^D**).

erase

Defines the erase character. When Line Mode is Off, typing the erase character erases one character. This value is in hexadecimal with a default value of **8** (ASCII value **^H**).

intr

Defines the interrupt character. Typing the interrupt character interrupts the current process. This value is in hexadecimal with a default value of **3** (ASCII value **^C**).

quit

Defines the quit character. Typing the quit character closes and exits the current telnet session. This value is in hexadecimal with a default value of **1c** (ASCII value **FS**).

escape

Defines the escape character. Returns you to the command line mode. This value is in hexadecimal with a default value of **1d** (ASCII value **GS**).

Set UDP

Description Configures the UDP settings for the serial line.

User Level Normal, Admin

Syntax

```
set udp line entry 1|2|3|4 [both|in|out|none <outbound_port>]
 [<start_ip_address>] [<end_ip_address>]
```

Options **both|in|out|none**

The direction in which information is received or relayed:

- **None**—UDP service not enabled.
- **In**—LAN to serial.
- **Out**—Serial to LAN.
- **Both**—Messages are relayed both directions.

<outbound_port>

The port that the Device Server will use to receive messages from or relay messages to servers/hosts.

<start_ip_address>

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

<end_ip_address>

The last host IP address in the range of IP addresses (for IPV4, not required for IPV6) that the Device Server will listen for messages from and/or send messages to.

Set Vmodem

Description Configures the vmodem settings for the serial line.

User Level Admin

Syntax

```
set vmodem line [failure-string <string>]
 [success-string <string>] [host <config_host>]
 [port <TCP_port>|0] [style numeric|verbose] [suppress on|off]
```

Options **failure-string**

String that is sent to the serial device when a connection fails. If no string is entered, then the string **`NO CARRIER`** will be sent.

success-string

String that is sent to the serial device when a connection succeeds. If no string is entered, then the string **`CONNECT`** will be sent with the connecting speed, for example **`CONNECT 9600`**.

host

The target host name.

port

The port number the target host is listening on for messages.

style

One of the following:

- **Verbose**—Return codes (strings) are sent to the connected device.
- **Numeric**—The following characters can be sent to the connected device:

  1 Successfully Connected

  2 Failed to Connect

  4 Error

suppress

If set to **No**, connection success/failure indication strings are sent to the connected device, otherwise these indications are suppressed.

Set Modbus-Slave Line

Description Sets the Modbus slave parameters for the line. SSL/TLS can be enabled and configured for this Line Service.

User Level Admin

Syntax

```
set modbus-slave line .|<number>|* [crlf on|off]
 [protocol rtu|ascii] [uid-range <uid_range>]
```

Options

crlf

When **Modbus/ASCII** is selected, adds a CR/LF to the end of the transmission; most Modbus devices require this option. The default is **On**.

protocol

Specify the protocol that is used between the Modbus Master(s) and Modbus Slave(s), either RTU or ASCII.

uid-range

You can specify a range of UIDs (1-247), in addition to individual UIDs. The format is comma delimited; for example, 2-35, 50, 100-103.

Set Modbus-Master Line

Description Sets the Modbus master parameters for the line. SSL/TLS can be enabled and configured for this Line Service.

User Level Admin

Syntax

```
set modbus-master line .|<number>|* [crlf on|off]
 [protocol rtu|ascii]
 [[entry <number> [port <port>] [protocol udp|tcp]
  [range-mode gateway|host] [slave-ip <IP_address>]
  [uid-range <start_uid> <end_uid>]]
```

Options

crlf

When **Modbus/ASCII** is selected, adds a CR/LF to the end of the transmission; most Modbus devices require this option. The default is **On**.

protocol

Specify the protocol that is used between the Modbus Master(s) and Modbus Slave(s), either RTU or ASCII.

entry

You can specify up to 16 Modbus Slave Remote IP Mapping entries (the UIDs must not overlap).

port

The destination port of the remote Modbus TCP Slave that the Device Server will connect to.

protocol

Specify the protocol that is used between the Modbus Master and Modbus Slave(s), either TCP or UDP.

range-mode

If you specify **Host**, the IP address is used for the first UID specified in the range. The last octect in the IPv4 address is then incremented for subsequent UID’s in that range. The **Host** option is not applicable for IPv6 addresses. If you specify **Gateway**, the Modbus Master Gateway will use the same IP address when connecting to all the remote Modbus slaves in the specified UID range.

slave-ip

The IP address of the TCP/Ethernet Modbus Slave.

uid-range

When **Range Mode** is **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 Device Server will automatically increment the last digit of the configured IP address. Therefore, you can specify a UID range of 1-100, and the Device Server will route Master Modbus messages to all Modbus Slaves with IP addresses of 10.10.10.1 - 10.10.10.100.

Show Interface

Description Shows the network interface information.

User Level Admin

Syntax

```
show interface [brief|ethernet]
```

Show Modbus

Description Shows the Modbus settings for a line.
User Level Admin
Syntax `show modbus master|slave <number>`

Show Telnet-Client

Description Shows the telnet client settings for a line.
User Level Admin
Syntax `show telnet-client`

Show UDP

Description Shows the UDP settings for the line.
User Level Admin
Syntax `show udp`

Show Vmodem

Description Show the vmodem settings for the line.
User Level Normal, Admin
Syntax `show vmodem`

Modem Commands

Add Modem

Description Adds a modem.
User Level Admin
Syntax `add modem <modem_name> <initialization_string>`

Options <***modem_name***>

The name of the modem. Do not use spaces.

<***initialization_string***>

The initialisation string of the modem; see your modem’s documentation.

Delete Modem

Description Deletes a modem.
User Level Admin
Syntax `delete modem <config_modem_name>`

Option <***config_modem_name***>

You can see a the list of modems that can be deleted by typing **`delete modem ?`**.

Show Modems

Description Shows the Device Server modem table.
User Level Normal, Admin
Syntax `show modems`

Packet Forwarding Commands

Set Packet-Forwarding Line

Description The Packet Forwarding feature allows you to control how the data coming from a serial device is packetized before forwarding the packet onto the LAN network. This command configures packet forwarding options for serial devices attached to the serial line. The command is broken up into the two logical flows that can be configured; if you configure both the packet options and the frame definition options, the frame definition options will take precedence. If any of the packet options that are configured are met, the packet transmission is triggered.

User Level Admin

Syntax

```
set packet-forwarding [enable-end-trigger1 on|off]
 [enable-end-trigger2 on|off] [end-trigger1 <0x0-FF>]
 [end-trigger2 <0x0-FF>] [force-transmit-timer <number>]
 [forwarding-rule trigger1|trigger+1|trigger+2|strip-trigger]
 [idle-timer <number>] [packet-size <number>]

set packet-forwarding [enable-eof1 on|off] [enable-eof2 on|off]
 [enable-sof1 on|off] [enable-sof2 on|off] [eof1 <0x0-FF>]
 [eof2 <0x0-FF>]
 [forwarding-rule trigger1|trigger+1|trigger+2|strip-trigger]
 [sof1 <0x0-FF>] [sof2 <0x0-FF>] [start-frame-transmit on|off]
```

Options

enable-end-trigger1

Enable or disable the end trigger1 hex character.

enable-end-trigger2

Enable or disable the end trigger2 hex character.

enable-end-eof1

Enable or disable the eof1 (end of frame) hex character.

enable-end-eof2

Enable or disable the eof2 (end of frame) hex character.

enable-end-sof1

Enable or disable the sof1 (start of frame) hex character.

enable-end-sof2

Enable or disable the sof2 (start of frame) hex character.

end-trigger1

When enabled, specifies the character that when received will define when the packet is ready for transmission. The actual transmission of the packet is based on the Trigger Forwarding Rule. Valid values are in hex 0-FF. The default is 0.

end-trigger2

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 Device Server waits for another End Trigger1 character to start the End Trigger1/End Trigger2 character sequence). The actual transmission of the packet is based on the Trigger Forwarding Rule. Valid values are in hex 0-FF. The default is 0.

eof1

Specifies the End of Frame character, which defines when the frame is ready to be transmitted. The actual transmission of the frame is based on the Trigger Forwarding Rule. Valid values are in hex 0-FF. The default is 0.

eof2

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 Device Server waits for another EOF1 character to start the EOF1/EOF2 character sequence), which defines when the frame is ready to be transmitted. The actual transmission of the frame is based on the Trigger Forwarding Rule. Valid values are in hex 0-FF. The default is 0.

force-transmit-timer

When the specified amount of time, in milliseconds, elapses after the first character is received from the serial port sender, the packet is transmitted. A value of zero (0) ignores this parameter. Valid values are 0-65535 ms. The default is 0.

forwarding-rule

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:

- **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.

idle-timer

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. Valid values are 0-65535 ms. The default is 0.

packet-size

The number of byte that must be received from the serial port before the packet is transmitted to the network. A value of zero (0) ignores this parameter. Valid values are 0-1024 bytes. The default is 0.

sof1

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. Valid values are in hex 0-FF. The default is 0.

sof2

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 Device Server waits for another SOF1 character to start the SOF1/SOF2 character sequence). Valid values are in hex 0-FF. The default is 0.

start-frame-transmit

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.

Show Packet-Forwarding Line

Description Shows the packet-forwarding settings for the line.
User Level Admin
Syntax **`show packet-forwarding line <`*`number`*`>`**

Network Commands

SNMP Commands

The Device Server supports SNMP traps restart and SNMP community authentication error.

Add Community

Description Adds an SNMP community (version 1 and version 2).
User Level Admin
Syntax

```
add community <community_name> <config_host>|<ip_address>
 none|readonly|readwrite
```

Options <***community_name***>

A name that will be sent to the Device Server from an SNMP manager. This name will define the permissions of the manager.

<***config_host***>|<***ip_address***>

The host name of the SNMP community that will send requests to the Device Server.

The IP address of the SNMP manager that will send requests to the Device Server. If the address is **`0.0.0.0`**, any SNMP manager with the **Community Name** can access the Device Server.

none|readonly|readwrite

Permits the Device Server to respond to SNMP requests by:

- **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.

Add Trap

Description Adds an SNMP trap.
User Level Admin
Syntax

```
add trap <trap_name> <config_host>|<ip_address>
```

Options <***trap_name***>

An arbitrary trap community name.

<***config_host***>|<***ip_address***>

Defines the hosts (by IP address) that will receive trap messages generated by the Device Server. Up to four trap hosts can be defined.

Delete Community

Description Deletes an SNMP community (version 1 and version 2).
User Level Admin
Syntax **`delete community <`***`config_community_number`***`>`**

Option <***config_community_number***>

When you add an SNMP community, it gets assigned to a number. To delete the SNMP community, you need to specify the number of the community that you want to delete. To see which community is assigned to what number, type the **`show snmp`** command.

Delete Trap

Description Deletes an SNMP trap.
User Level Admin
Syntax **`delete trap <`***`config_trap_number`***`>`**

Option <***config_trap_number***>

When you add an SNMP trap, it gets assigned to a number. To delete the SNMP trap, you need to specify the number of the trap that you want to delete. To see which trap is assigned to what number, type the **`show snmp`** command.

Set SNMP

Description Configures SNMP settings.
User Level Admin
Syntax

```
set snmp [contact <string>] [location <string>]
 [readonly user <username>] [readwrite user <username>]
```

Options **contact**

The name and contract information of the person who manages this SMNP node.

location

The physical location of the SNMP node.

readonly user

(SNMP version 3) Specified user can only view SNMP variables.

readwrite user

(SNMP version 3) Specified user can view and edit SNMP variables.

Show SNMP

Description Shows SNMP settings, including communities and traps.
User Level Admin
Syntax **`show snmp`**

TFTP Commands

Set Server TFTP

Description Configures the Device Server's TFTP client settings.
User Level Admin
Syntax **`set server tftp [retry <`*`integer`*`>] [timeout <`*`integer`*`>]`**

Options **retry**

The number of times the Device Server will attempt to transfer (using TFTP) a file to/from a host. Enter a value between 0 and 5. The default is **5**. A value of **0** (zero) means that the Device Server will not attempt a retry should TFTP fail.

timeout

The time, in seconds, that the Device Server will wait for a successful transmit or receipt of TFTP packets before retrying a TFTP transfer. Enter a value between 3 and 10. The default is **3** seconds.

Hosts Commands

Add Host

Description Adds a host to the Device Server host table.
User Level Admin
Syntax **`add host <hostname> <ip_address>`**

Options <***hostname***>

The name of the host.

<***ip_address***>

The host IP address.

Delete Host

Description Deletes a host from the Device Server host table.
User Level Admin
Syntax **`delete host <config_host>`**

Option <***config_host***>

You can see a list of hosts that can be deleted by typing **`delete host ?`**.

Set Host

Description Configures a host in the Device Server host table.
User Level Admin
Syntax **`set host <config_host> <ip_address>`**

Options <***config_host***>

The name of the host.

<***ip_address***>

The host IP address.

Show Hosts

Description Shows the Device Server host table.
User Level Normal, Admin
Syntax **`show hosts`**

Gateway Commands

Add Gateway

Description Adds a gateway. You can configure up to twenty gateways.

User Level Admin

Syntax

```
add gateway <config_host> default

add gateway <config_host> host <dest_ip_addr>

add gateway <config_host> network
 <dest_IPv4_addr>|<dest_IPv6_addr>
 [<subnet_bits_0-32>|<subnet_bits_0-128>]
```

Options *<config_host>*

You can specify up to twenty hosts to act as gateways in your network. Each gateway host must be defined in the Device Server host table.

default|host|network

Specify the type of gateway:

- **Default**—A gateway which provides general access beyond your local network.
- **Host**—A gateway reserved for accessing a specific host external to your local network.
- **Network**—A gateway reserved for accessing a specific network external to your local network.

<dest_IP_addr>

When the gateway is a **Host** or **Network** gateway, you must specify the IP address of the target host machine/network.

<subnet_bits>

When the gateway is a **Network** gateway, you must specify the network's subnet mask.

Delete Gateway

Description Deletes a gateway.

User Level Admin

Syntax `delete gateway <config_gateway_host>`

Option *<config_gateway_host>*

You can view the configured gateways that can be deleted by typing `delete gateway ?`.

Set Gateway

Description Configures the gateway.
User Level Admin
Syntax

```
set gateway <config_gateway_host> default

set gateway <config_gateway_host> host <destination_ip>

set gateway <config_gateway_host>
 network <dest_IPv4_addr>|<dest_IPv6_address>
 [<subnet_bits_0-32>|<subnet_bits_0-128>]
```

Options <***config_gateway_host***>

You can view the configured gateways that can be deleted by typing `delete gateway ?`.

default|host|network

Specify the type of gateway:

- **Default**—A gateway which provides general access beyond your local network.
- **Host**—A gateway reserved for accessing a specific host external to your local network.
- **Network**—A gateway reserved for accessing a specific network external to your local network.

<***dest_IP_addr***>

When the gateway is a **Host** or **Network** gateway, you must specify the IP address of the target host machine/network.

<***subnet_bits***>

When the gateway is a **Network** gateway, you must specify the network's subnet mask.

Show Gateways

Description Shows configured gateways.
User Level Normal, Admin
Syntax `show gateways`

Logging Commands

Set Syslog

Description Configures the system log.
User Level Admin
Syntax

```
set syslog
 [level emergency|alert|critical|error|warning|notice|info|debug]
 [primary-host <config_host>] [secondary-host <config_host>]
```

Options **level**

Choose the event level that triggers a syslog entry:

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

When you select a **Level**, all the levels that appear above it in the list also trigger a syslog entry. For example, if you select **Error**, all **Error**, **Critical**, **Alert**, and **Emergency** events will be logged.

primary-host

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

secondary-host

If the Device Server cannot communicate with the primary host, then the Device Server will attempt to send system log messages to this preconfigured host; messages will be displayed on the host's monitor.

Show Syslog

Description Shows the syslog settings.
User Level Admin
Syntax `show syslog`

Time Commands

Set Time

Description Sets the Device Server's system clock.
User Level Admin
Syntax `set time <hh:mm[:ss]>`

Option <***hh***:***mm***[:***ss***]>

Sets the Device Server's system time, using military time format.

Show Time

Description Shows the Device Server's system clock.
User Level Normal, Admin
Syntax `show time`

Time/Date Setting Commands

Set Date

Description Sets the Device Server's system clock.
User Level Admin
Syntax **`set date <`***`dd/mm/yyyy`***`>`**

Set Time

Description Sets the Device Server's system clock.
User Level Admin
Syntax **`set time <`***`hh`***`:`***`mm`***`[:`***`ss`***`]>`**

Option <***hh***:***mm***[:***ss***]>

Sets the Device Server's system time, using military time format.

Show Date

Description Shows the date, according to the Device Server system clock.
User Level Normal, Admin
Syntax **`show date`**

Show Time

Description Shows the Device Server's system clock.
User Level Normal, Admin
Syntax **`show time`**

Administration Commands

Bootup Commands

Reboot

Description Reboots the Device Server. You will be prompted to save configuration to FLASH, if there have been unsaved configuration changes.
User Level Admin
Syntax **`reboot`**

Reset

Description Resets the user profile or serial line to the default factory configuration.
User Level Admin
Syntax **`reset user .|<`***`username`***`>|*`**

`reset line`

Reset Factory

Description Resets the Device Server to the factory configuration.
User Level Admin
Syntax **`reset factory`**

Save

Description Saves the configuration to FLASH.
User Level Admin
Syntax **`save`**

Set Bootup

Description Specifies remote the TFTP host and pathname for files to be loaded after a Device Server reboot.

User Level Admin

Syntax

```
set bootup firmware host <hostname> [file <path_filename>]

set bootup configuration host <hostname> [file <path_filename>]
```

Options

firmware file

The path and file name (do not use a drive letter), relative to the default path of your TFTP server software, of the update software for the Device Server that will be loaded when the Device Server is rebooted.

configuration file

The path and file name (do not use a drive letter), relative to the default path of your TFTP server software, of the configuration software for the Device Server that will be loaded when the Device Server is rebooted.

host

The host name or IP address of the server that contains the configuration or firmware file. If you use a host name, it must exist in the Device Server's host table or be resolved by DNS.

Show ARP

Description Shows the current contents of the ARP cache.

User Level Admin

Syntax

```
show arp
```

Show Bootup

Description Shows the Firmware and Configuration files specified for Device Server bootup.

User Level Admin

Syntax

```
show bootup
```

TFTP File Transfer Commands

Netload

Description Transfers a file from a remote host to the Device Server using the TFTP protocol.

User Level Admin

Syntax

```
netload firmware|configuration|customlang|term1|term2|term3
 <hostname/ip_address> <filename>
```

Options

firmware

Specifies that you are going to download a new firmware file to the Device Server.

configuration

Specifies that you are going to download a new configuration file to the Device Server.

customlang

Specifies that you are going to download a custom language file to the Device Server.

term1|term2|term3

You can create and download up to three custom terminal definitions to the Device Server.

<hostname/ip_address>

The IP address or host name where the file you are downloading to the Device Server resides. If you are using a host name, it must be resolved in either the Device Server's **Host Table** or a DNS server.

<filename>

The complete path and file name (cannot use a drive letter) of the file you are downloading to the Device Server.

Netsave

Description Transfers a file from the Device Server to a remote host using the TFTP protocol.
User Level Admin
Syntax `netsave configuration|crash <hostname/ip_address> <filename>`

Options **configuration**

Specifies that you are going to upload a configuration file from the Device Server to the specified host or IP address.

crash

Specifies that you are going to upload a crash file from the Device Server to the specified host or IP address.

<hostname/ip_address>

The IP address or host name for where the file you are uploading from the Device Server is going. If you are using a host name, it must be resolved in either the Device Server's **Host Table** or a DNS server.

<filename>

The complete path and file name (cannot use a drive letter) for the file you are uploading from the Device Server.

MOTD Commands

Set MOTD

Description Specifies the server/file that contains the message of the day (MOTD) that is displayed when users log into the Device Server.
User Level Normal, Admin
Syntax `set motd host <hostname> file <path_filename>`

Options **host**

The host that the Device Server will be getting the Message of the Day file from.

file

The path and file name (do not use a drive letter), 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 Device Server.

Show MOTD

Description Show the Message of the Day (MOTD) settings.
User Level Admin
Syntax `show motd`

Statistic Commands

Configuration Statistics

Show Netstat

Description Shows currently used TCP/UDP sockets/ports.
User Level Admin
Syntax `show netstat [all] [listening] [tcp] [udp] [tcpv6] [updv6]`
Options **all**

Displays all ports, including server (listening) ports; by default, listening ports are not displayed.

listening

Displays server (listening) ports; by default, listening ports are not displayed.

tcp

Displays TCP port statistics.

udp

Displays UDP port statistics.

tcpv6

Displays TCPv6 port statistics.

udpv6

Displays UDPv6 port statistics.

Show Modbus Statistics

Description Shows the Modbus statistics.
User Level Admin
Syntax

```
show modbus statistics master-tcp line *|<number>

show modbus statistics master-udp line  *|<number>

show modbus statistics slave-tcp line  *|<number>

show modbus statistics slave-udp line *|<number>
```

Show Netstat Statistics

Description Shows protocol (IP/ICMP/TCP/UDP) counters.
User Level Admin
Syntax `show netstat statistics [ip] [ipv6] [icmp] [icmpv6] [tcp] [udp] [udp6]`

Show Routes

Description Shows current information about IPv4 or IPv6 network routes.
User Level Admin
Syntax `show routes [ipv6]`

Run-Time Statistics

Delete Arp

Description Delete entries from the Device Server's ARP cache. Takes effect immediately; not related to configuration.
User Level Admin
Syntax **`delete arp`**

Show Arp

Description Shows the current contents of the ARP cache.
User Level Admin
Syntax **`show arp`**

Show Serial

Description Shows statistics on the serial port.
User Level Admin
Syntax **`show serial`**

Uptime

Description Displays the elapsed time (in days, hours, minutes, and seconds) since the last reboot/power cycle.
User Level Admin
Syntax **`uptime`**

A Troubleshooting

Introduction

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

Hardware Problems

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

- If the Device Server is not in Console mode, do the following:

  a. Set up a direct connection to the Device Server; see ***Using a Direct Connection*** on page 24 for information on this type of connection.

  b. Power the Device Server off.

  c. Switch the Console dip switch to On.

  d. Power the Device Server on.

  If there is a problem with the Device Server firmware, you will need to reload the firmware, which can be found either on the CD-ROM that came with the Device Server.
- If the Device Server is already in Console mode and the Power LED stays red, you need to make arrangements to return the Device Server.

If you purchased the Device Server less than 30 days before this problem appears, contact your distributor.

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*** on page 27 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 Device Server, *reboot* the Device Server (does not apply when using BOOTP or DHCP). Once the Device 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 Device Server, verify that the **Server Services HTTP** and/or **HTTPS** are 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 Device 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 Device Server to its factory default settings using the **Reset** switch on the rear panel. There is no procedure to access the Device Server without a password.

Problems with Terminals

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

The Device 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 Device Server's port.

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

- Set your **Line** to **`Termtype`** VT100, ANSI or WYSE60 (or other form of terminal emulation, if you have downloaded one). The default line type in the Device 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 Device 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 Device 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 Device Server already configured and you do know your password, but have lost, misconfigured, or don't know the IP address of the Device Server, and you cannot obtain a login.

- If the Device Server resides within the local network segment, you can use DeviceManager to find the Device Server.
- You can connect directly to the serial port of the Device Server, as explained in ***Using a Direct Connection*** on page 24.

DHCP/BOOTP Problems

Messages: `host name too long` or `filename too long`.

- The Device 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 Device 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 Device 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 Device 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 customised 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 Device Server takes a long time.

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

B Utilities

Introduction

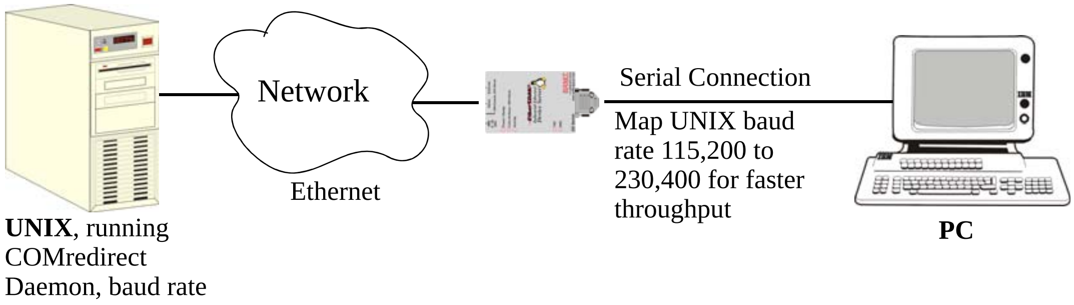
This chapter provides information on the COMredirect utility.

COMredirect

COMredirect is a com port redirector utility for the Device 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 Device Server.

You use COMredirect when you want to connect extra terminals to a server using a Device Server rather than a multi-port serial card. COMredirect is especially useful when you want to improve security, for example, to see which user is logged onto which terminal. 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.


Network
Ethernet
Serial Connection
Map UNIX baud rate 115,200 to 230,400 for faster throughput
UNIX, running COMredirect Daemon, baud rate
PC

Currently, COMredirect is supported on:

- Solaris (x86) 2.6, 2.7, 2.8, 2.9
- SCO Unixware 7 (and SCO Open UNIX 8)
- SCO OpenServer 5.0x
- LINUX
- Windows 2000/Server 2003/NT/XP

For more information, see the *COMredirect User Guide* on the CD-ROM.

Glossary

This chapter provides definitions for Device 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.

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 Device Server enabling the user to log straight into a specific host. A direct connection is recommended where a user logging in to the Device 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.

Local Authentication Uses the user ID and password stored within the Device Server User database.

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 Device 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.

Reverse Connection Connections that originate from a host that go directly to a serial device through the Device Server.

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 redisplays 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.

Index