SecureBox

SDS1100
User Guide

Part Number 900-354
Revision A April 2004

Copyright & Trademark

Contacts

Lantronix
15353 Barranca Parkway
Irvine, CA 92618, USA
Phone: 949-453-3990
Fax: 949-453-3995

Technical Support
Phone: 800-422-7044 or 949-453-7198
Fax: 949-450-7226
Online: www.lantronix.com/support
E-mail support@lantronix.com

Sales Offices
For a current list of our domestic and international sales offices, go to the Lantronix web site at http://www.lantronix.com/about/contact/index.html

Disclaimer & Revisions

Operation of this equipment in a residential area is likely to cause interference in which case the user, at his or her own expense, will be required to take whatever measures may be required to correct the interference.

Note: *This product has been designed to comply with the limits for a Class A digital device pursuant to Part 15 of FCC Rules. These limits are designed to provide reasonable protection against such interference when operating in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with this guide, may cause harmful interference to radio communications.*

Changes or modifications to this device not explicitly approved by Lantronix will void the user's authority to operate this device.

The information in this guide may change without notice. The manufacturer assumes no responsibility for any errors that may appear in this guide.

Note: *Export Control Classification Number 5A002, License exception ENC. The following export agreement is required for encryption:*

I agree that I will not export or re-export this product or firmware to a national resident of Cuba, Iran, Iraq, Libya, North Korea, Sudan, Syria or any other country to which the United States has embargoed goods; or to anyone on the US Treasury Department's list of Specially Designated Nationals and Blocked Persons, US Commerce Department's Table of Denial Orders and Entitles List, or the US State Department's Debarred List. By receiving this product, I am agreeing to the foregoing and I am representing and warranting that I am not located in, under the control of, or a national or resident of any such country or on any such list.

Date	Part No.	Rev.	Comments
4/04	900-354	A	Initial Document

Declaration of Conformity

(according to ISO/IEC Guide 22 and EN 45014)

Manufacturer's Name & Address:

Lantronix 15353 Barranca Parkway, Irvine, CA 92618 USA

Declares that the following product:

Product Name Model: SecureBox Device Server SDS1100

Conforms to the following standards or other normative documents:

Safety: EN60950:1992+A1, A2, A3, A4, A11

Electromagnetic Emissions:

EN55022: 1994 (IEC/CSPIR22: 1993)

FCC Part 15, Subpart B, Class B

IEC 1000-3-2/A14: 2000
IEC 1000-3-3: 1994

Electromagnetic Immunity:

EN55024: 1998 Information Technology Equipment-Immunity Characteristics

IEC61000-4-2: 1995 Electro-Static Discharge Test
IEC61000-4-3: 1996 Radiated Immunity Field Test
IEC61000-4-4: 1995 Electrical Fast Transient Test
IEC61000-4-5: 1995 Power Supply Surge Test
IEC61000-4-6: 1996 Conducted Immunity Test
IEC61000-4-8: 1993 Magnetic Field Test
IEC61000-4-11: 1994 Voltage Dips & Interrupts Test

(L.V.D. Directive 73/23/EEC)

Supplementary Information:

This Class A digital apparatus complies with Canadian ICES-003 (CSA) and has been verified as being compliant within the Class A limits of the FCC Radio Frequency Device Rules (FCC Title 47, Part 15, Subpart B CLASS A), measured to CISPR 22: 1993 limits and methods of measurement of Radio Disturbance Characteristics of Information Technology Equipment. The product complies with the requirements of the Low Voltage Directive 72/23/EEC and the EMC Directive 89/336/EEC.

Encryption: This product includes AES encryption certified by the National Institute of Standard and Technology to FIPS-197 standard certification #120.

Export Control Classification Number 5A002, License exception ENC.

Manufacturer's Contact:

Director of Quality Assurance, Lantronix
15353 Barranca Parkway, Irvine, CA 92618 USA
Tel: 949-453-3990
Fax: 949-453-3995

Warranty

Lantronix warrants each Lantronix product to be free from defects in material and workmanship for a period of **TWO YEARS** after the date of shipment. During this period, if a customer is unable to resolve a product problem with Lantronix Technical Support, a Return Material Authorization (RMA) will be issued. Following receipt of an RMA number, the customer shall return the product to Lantronix, freight prepaid. Upon verification of warranty, Lantronix will -- at its option -- repair or replace the product and return it to the customer freight prepaid. If the product is not under warranty, the customer may have Lantronix repair the unit on a fee basis or return it. No services are handled at the customer's site under this warranty. This warranty is voided if the customer uses the product in an unauthorized or improper way, or in an environment for which it was not designed.

Lantronix warrants the media containing its software product to be free from defects and warrants that the software will operate substantially according to Lantronix specifications for a period of **60 DAYS** after the date of shipment. The customer will ship defective media to Lantronix. Lantronix will ship the replacement media to the customer.

* * * *

In no event will Lantronix be responsible to the user in contract, in tort (including negligence), strict liability or otherwise for any special, indirect, incidental or consequential damage or loss of equipment, plant or power system, cost of capital, loss of profits or revenues, cost of replacement power, additional expenses in the use of existing software, hardware, equipment or facilities, or claims against the user by its employees or customers resulting from the use of the information, recommendations, descriptions and safety notations supplied by Lantronix. Lantronix liability is limited (at its election) to:

refund of buyer's purchase price for such affected products (without interest)

repair or replacement of such products, provided that the buyer follows the above procedures.

There are no understandings, agreements, representations or warranties, express or implied, including warranties of merchantability or fitness for a particular purpose, other than those specifically set out above or by any existing contract between the parties. Any such contract states the entire obligation of Lantronix. The contents of this document shall not become part of or modify any prior or existing agreement, commitment or relationship.

For details on the Lantronix warranty replacement policy, go to our web site at http://www.lantronix.com/support/warranty/index.html

Contents

1: Introduction

Features

The SecureBox family of Secure Device Servers (SDS) allows serial devices such as those listed below to securely connect and communicate over Ethernet networks using the IP protocol family (TCP for connection-oriented stream applications and UDP for datagram applications).

- Security Alarms
- Access Control Devices
- Fire Control Panels
- Time/Attendance Clocks and Terminals
- ATM Machines
- Data Collection Devices
- RFID readers
- Universal Power Supply (UPS) Management Units
- Telecommunications Equipment
- Data Display Devices

Protocol Support

The SDS1100 uses the Internet Protocol (IP) for network communications and the Transmission Control Protocol (TCP) to assure that no data is lost or duplicated, and that everything sent to the connection arrives correctly at the target.

Other supported protocols are listed below:

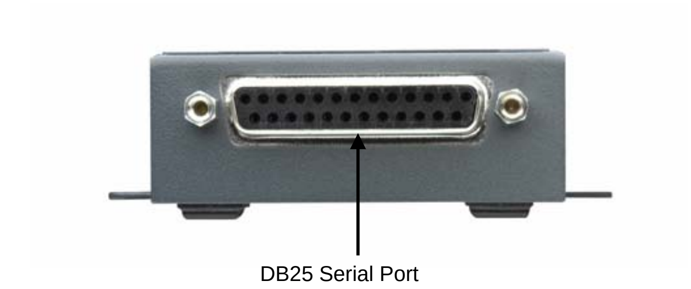
- ARP, UDP, TCP, ICMP, Telnet, TFTP, AutoIP, DHCP, HTTP, and SNMP for network communications.
- TCP, UDP, and Telnet for connections to the serial port.
- TFTP for firmware updates.
- IP for addressing, routing, and data block handling over the network.
- User Datagram Protocol (UDP) for typical datagram applications in which devices interact with other devices without maintaining a point-to-point connection.

Connections and Pinouts

Serial Port

The unit has a female DCE DB25 serial port that supports RS-232 and RS-485/422 serial standards (software selectable) up to 115 Kbps.

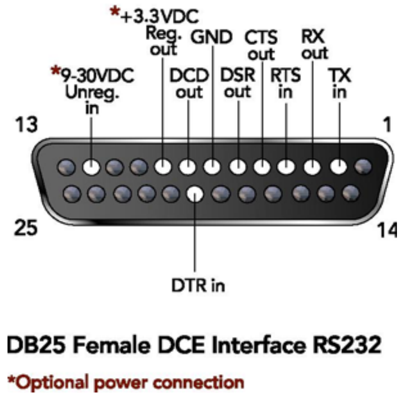
Figure 1-1. Serial Interface

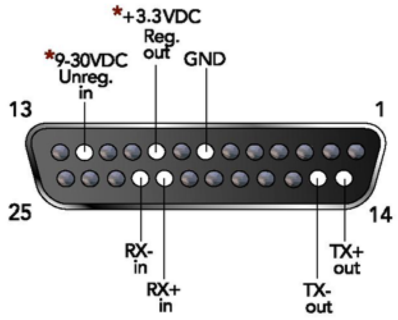


Serial Connector Pinouts

The unit’s female DB25 connector provides an RS-232C, RS-485, or RS-422 DCE serial port. The default serial port settings are 9600 baud, 8 bits, no parity, and 1 stop bit.

Figure 1-2. DB25F DCE Serial Connector





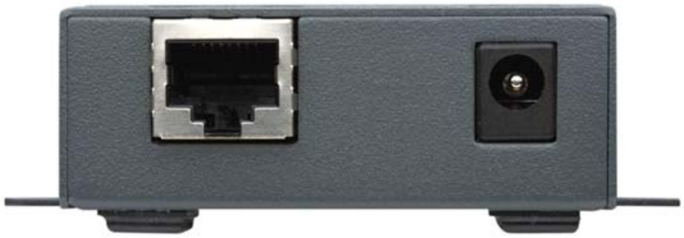
DB25 Female DCE Interface RS485/422

*Optional power connection

Network Port

The unit's back panel contains a 9-30VDC power plug and an RJ45 (10/100) Ethernet port.

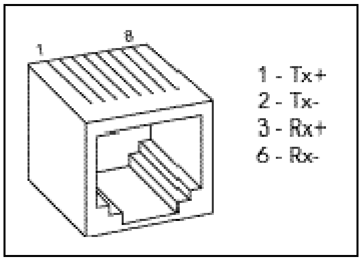
Figure 1-3. Network Interface



Ethernet Connector Pinouts

The unit supports 10 Mbps Ethernet through an RJ45 connector.

Figure 1-4. RJ45 Ethernet Connector



LEDs

The unit contains the following LEDs:

- 10 Mbps Link/Activity (green)
- 100 Mbps Link/Activity (green)
- Collisions
- Diagnostics (red)
- Status (yellow)

Simultaneously lit red and green LEDs mean something is wrong. If the red LED is lit or blinking, count the number of times the green LED blinks between its pauses. The following table explains the LED functions:

Table 1-1. SDS1100 LEDs

Serial LEDs	Meaning
10 Mbps link/activity steady green	Valid 10 Mbps network connection
10 Mbps link/activity blinking	Network packets transmitting and receiving
100 Mbps link/activity steady green	Valid 100 Mbps network connection
100Mbps link/activity blinking	Network packets transmitting and receiving
Collision blinking red	Network collisions
Diagnostic steady red and status blinking green	2 blinks = RAM error 4 blinks = EEPROM checksum error 5 blinks = Duplicate IP address on network
Diagnostic blinking red and status blinking green	5 blinks = No DHCP response
Status steady green	Serial port not connected to network
Status blinking green	Serial port connected to network

Product Information Label

The product information label on the underside of the unit contains the following information about your specific unit:

- Bar Code
- Serial Number
- Product ID (name)
- Product Description
- Ethernet Address (also referred to as Hardware Address or MAC Address)

Technical Specifications

CPU, Memory	Lantronix DSTni-LX 186 CPU, 48 MHz 1 MByte FLASH ROM 256 Kbytes zero wait state RAM
Serial Interface	Female DB25 connector (DCE pinout) Speed software selectable (300 to 115 kBaud) Software selectable RS-232C or RS-422/485
Network Interface	10/100 RJ45 Ethernet
Power Supply	External adapter included 120VAC USA 100 - 240 VAC Universal with regional connectors
Power Input	9-30 VDC or 9-24 VAC (1W maximum)
Dimensions	Height: 2.3 cm (0.9 in) Width: 6.4 cm (2.5 in) Depth: 9.0 cm (3.5 in)
Weight	0.35 Kg (0.8 lbs)
Temperature	Operating range: 5° to 50° C (41° to 122° F) Storage range: -40° to 66° C (-40° to 151° F)
Relative Humidity	Operating: 10% to 90% non-condensing, 40% to 60% recommended Storage: 10% to 90% non-condensing

2: Getting Started

Addresses and Port Number

Ethernet (MAC) Address

The Ethernet address is also referred to as the hardware address or the MAC address. The first three bytes of the Ethernet Address are fixed and read 00-20-4A, identifying the unit as a Lantronix product. The fourth, fifth, and sixth bytes are unique numbers assigned to each unit.

Figure 2-1. Sample Ethernet Address

00-20-4A-14-01-18 or 00:20:4A:14:01:18

Internet Protocol (IP) Address

Every device connected to an IP network must have a unique IP address. This address is used to reference the specific unit.

Port Number

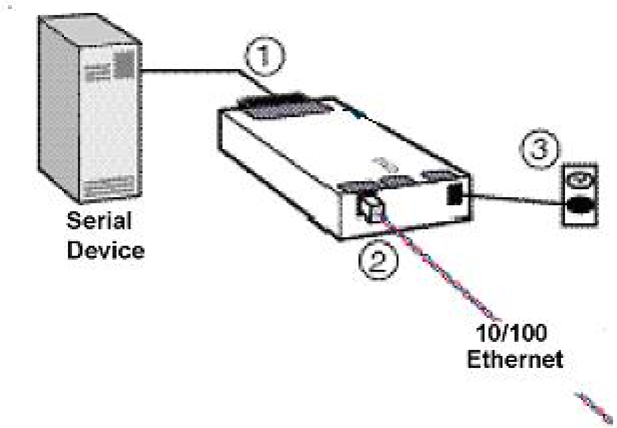
Every TCP connection and every UDP datagram is defined by a destination IP address and a port number. For example, a Telnet application commonly uses port number 23. A port number is similar to an extension on a PBX system.

The unit’s serial channel (port) can be associated with a specific TCP/UDP port number. Port number 9999 is reserved for access to the unit's Setup (configuration) Mode window.

Physically Connecting the Unit

The following diagram shows a properly installed unit:

Figure 2-2. SDS1100 Connected to Serial Device and Network



To install the unit, complete the following steps in order. Refer to the numbers in the previous figure.

1. Connect a serial device to your unit. See *Connections and Pinouts* in the Introduction for more information about what kinds of device attachments the unit supports.

2. Connect an Ethernet cable to the 10/100 port.

3. Supply power to your unit using the power supply that was included in the packaging.

   Note: *The required input voltage is 9-30 VDC or 9-24 VAC (1 W maximum).*

4. Supply power to the serial device.

Methods of Assigning the IP Address

The unit's IP address must be configured before a network connection is available. You have the following options for assigning an IP to your unit:

Method	Description
DHCP	A DHCP server automatically assigns the IP address and network settings.
DeviceInstaller	You manually assign the IP address using a graphical user interface (GUI). You must use a PC and the unit must be attached to the local network.
ARP and Telnet	You manually assign the IP address and other network settings at a command prompt using a UNIX or Windows-based system. Only one person at a time can be logged into the configuration port (port 9999). This eliminates the possibility of several people simultaneously attempting to configure the unit.
AutoIP	This automatic method is appropriate when you have a small group of hosts rather than a large network. This method allows the hosts to negotiate with each other and assign addresses, in effect creating a small network.
Serial Port Login	You initially configure the unit through a serial connection.

These methods are described in the remaining sections of this chapter.

Note: *In most installations, a fixed IP address is desirable. The systems administrator generally provides the IP address. Obtain the following information before starting to set up your unit:*

IP Address ___ ___ ___ ___

Subnet Mask: ___ ___ ___ ___

Gateway: ___ ___ ___ ___

DHCP

The unit ships with a default IP address of 0.0.0.0, which automatically enables DHCP.

Provided a DHCP server exists on the network, it will provide the unit with an IP address, gateway address, and subnet mask when the unit boots up. The SDS1100 has acquired an IP address if the red LED stops flashing and the green Status LED is on continuously. (If no DHCP server exists, the unit responds with a diagnostic error: the red Diagnostic LED blinks continuously, and the green Status LED blinks five times. This blinking only continues for about 15 seconds.)

You can use the DeviceInstaller software to search the network for the IP your unit has been assigned by the DHCP server and add it to the managed list. See *Add the Unit to the Manage List* later in this chapter.

Note: *This DHCP address will* ***not*** *appear in the unit's standard configuration screens. You can, however, determine your unit's DHCP-assigned IP address in Monitor Mode. When you enter Monitor Mode from the serial port with network connection enabled (see Monitor Mode in the Troubleshooting chapter) and issue the* ***NC*** *(Network Communication) command, you will see the unit's IP configuration.*

AutoIP

The unit ships with a default IP address of 0.0.0.0, which automatically enables Auto IP within the unit. AutoIP is an alternative to DHCP that allows hosts to automatically obtain an IP address in smaller networks that may not have a DHCP server. A range of IP addresses (from 169.254.0.1 to 169.254.255.1) has been explicitly reserved for AutoIP-enabled devices. The range of Auto IP addresses is **not** to be used over the Internet.

If your unit cannot find a DHCP server, and you have not manually assigned an IP address to it, the unit automatically selects an address from the AutoIP reserved range. Then, your unit sends out a (ARP) request to other nodes on the same network to see whether the selected address is being used.

- If the selected address is not in use, then the unit uses it for local subnet communication.
- If another device is using the selected IP address, the unit selects another address from the AutoIP range and reboots itself. After reboot, the unit sends out another ARP request to see if the selected address is in use, and so on.

AutoIP is not intended to replace DHCP. The unit will continue to look for a DHCP server on the network. If a DHCP server is found, the unit will switch to the DHCP server-provided address and reboot.

Note: *If a DHCP server is found, but it denies the request for an IP address, the unit does not attach to the network, but waits and retries.*

AutoIP can be disabled by setting the unit's IP address to 0.0.1.0. This setting enables DHCP but disables AutoIP.

DeviceInstaller

You can manually assign the IP address using the DeviceInstaller, which is on the product CD.

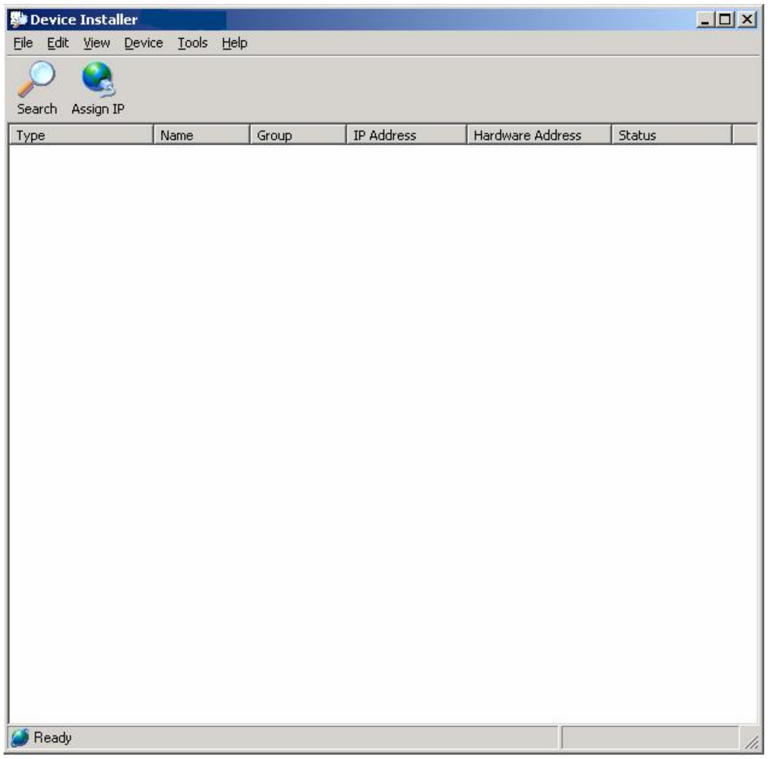
Install the DeviceInstaller

1. Insert the product CD into your CD-ROM drive. The Lantronix SDS1100 DeviceServer window displays.
2. If the CD does **not** launch automatically:
3. Click the **Start** button on the Task Bar and select **Run**.
4. Enter your CD drive letter, colon, backslash, **deviceinstaller.exe** (e.g., **E:\deviceinstaller.exe**).
5. Click the **DeviceInstaller** button. The installation wizard window displays.
6. Respond to the installation wizard prompts. (When prompted to select an installation type, select **Typical**.)

Assign IP Address and Network Class

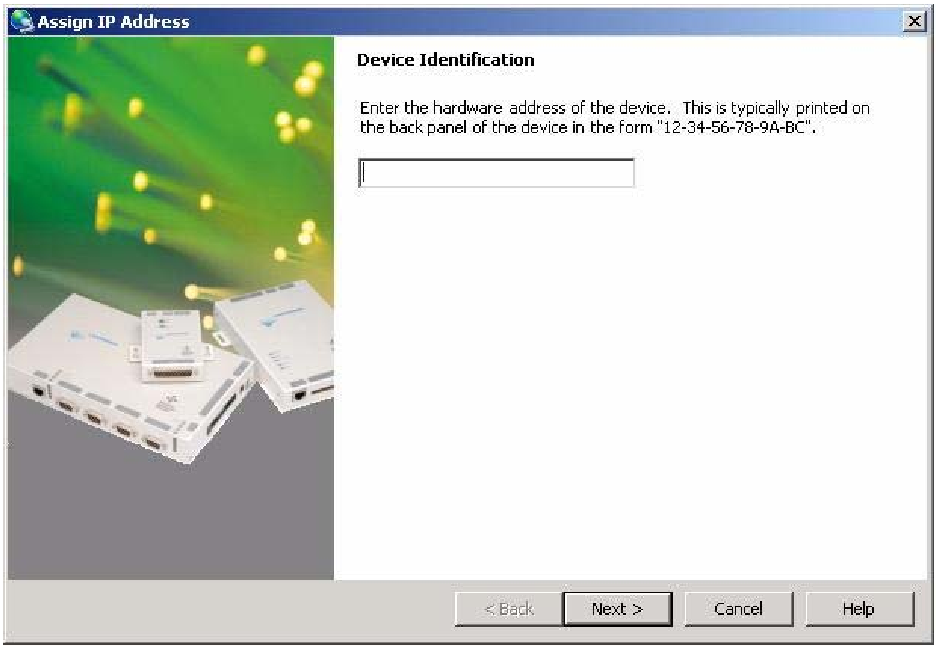
1. Click the **Start** button on the Task Bar and select **Programs → Lantronix → Device Installer → Device Installer**. The DeviceInstaller window displays.

Figure 2-3. DeviceInstaller Window



2. Click the **Assign IP** icon . The **Assign IP Address** window displays.

Figure 2-4. Assign IP Address Window (Device Identification)



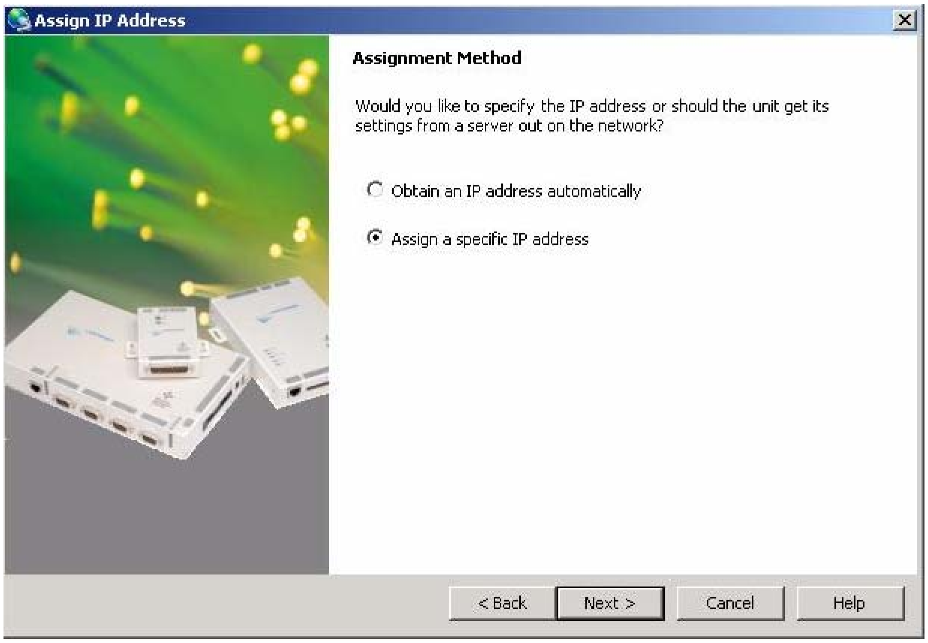
Assign IP Address

Device Identification

Enter the hardware address of the device. This is typically printed on the back panel of the device in the form "12-34-56-78-9A-BC".

3. Enter the Hardware or Ethernet address of the device. The following Assign IP Address window appears.

Figure 2-5. Assign IP Address Window (Assignment Method)



Assign IP Address

Assignment Method

Would you like to specify the IP address or should the unit get its settings from a server out on the network?

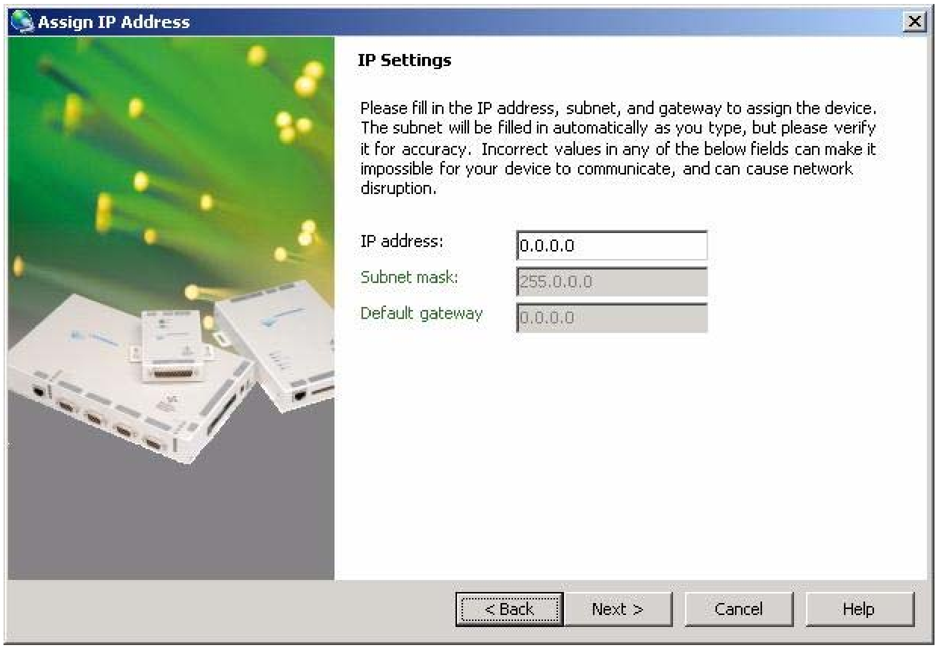
○ Obtain an IP address automatically

● Assign a specific IP address

4. Select **Assign a specific IP address** to assign a static IP address to the device or select **Obtain an IP address automatically** to enable BOOTP, DHCP, or Auto IP on the device.

5. Click **Next**. The following Assign IP Address window appears.

Figure 2-6. Assign IP Address Window (IP Settings)



Assign IP Address

IP Settings

Please fill in the IP address, subnet, and gateway to assign the device. The subnet will be filled in automatically as you type, but please verify it for accuracy. Incorrect values in any of the below fields can make it impossible for your device to communicate, and can cause network disruption.

IP address: 0.0.0.0

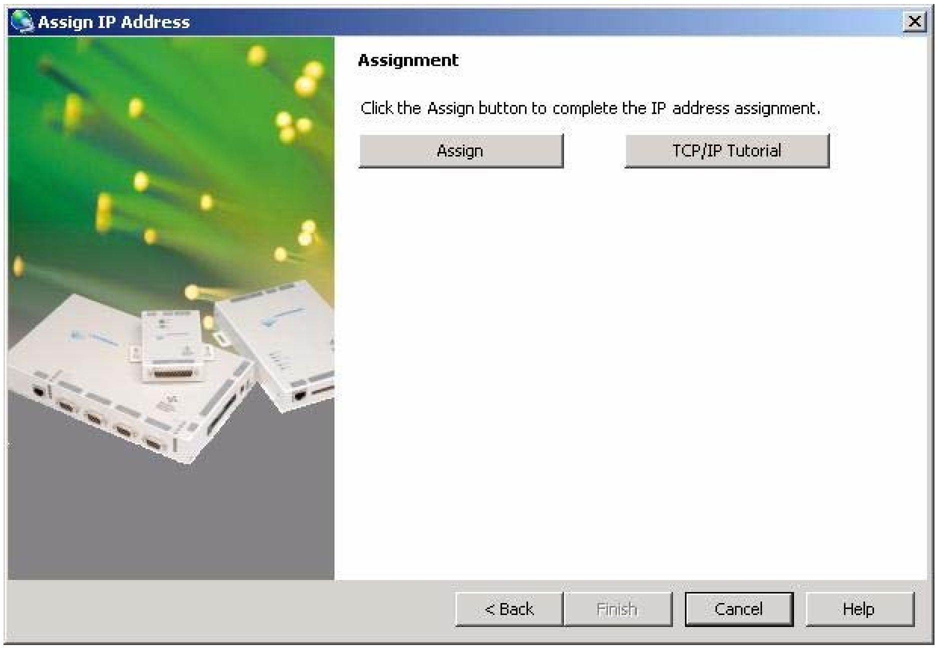
Subnet mask: 255.0.0.0

Default gateway 0.0.0.0

6. Enter the IP address, subnet mask, and gateway being assigned to the device. Enter this information in **XXX.XXX.XXX.XXX** format.

7. Click **Next**. The following Assign IP Address window appears.

Figure 2-7. Assign IP Address Window (Assignment)



Assignment

Click the Assign button to complete the IP address assignment.

8. Click the **Assign** button to finalize the IP assignment.

Add the Unit to the Manage List

Now add the unit to the list of similar Lantronix devices on the network so that you can manage and configure it. To perform this step, click the **Search** icon:

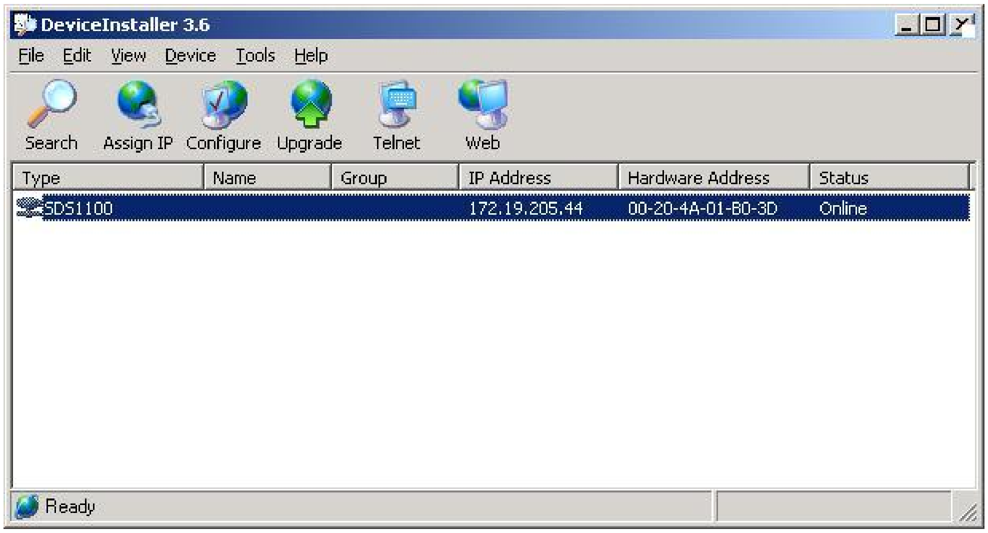
Search

The device should be located by DeviceInstaller and added into the Device List. Now you can manage (configure) the unit so that it works with the serial device on the network.

Opening a Configuration Window

Once the device is added into the list, use the **Configure**, **Upgrade, Telnet**, or **Web** icons to manage the device.

Figure 2-8. Device Management Window



Type	Name	Group	IP Address	Hardware Address	Status
SDS1100			172.19.205.44	00-20-4A-01-B0-3D	Online

1. Do *one* of the following:

   Note: *To assign Expert settings and Security settings, you must use the Setup Mode window in a Telnet session.*

   - To configure the unit via a Web browser, click the **Web** icon. The Lantronix WEB-Manager window displays in your browser.
   - To configure the unit via a Telnet session, click the **Telnet** icon. The Setup Mode window displays.

2. Continue with the appropriate configuration procedure described in the next chapter.

   Note: *The **Configure** icon on the Device Management window allows you to save a configuration locally on your computer as a file. It is helpful to save the file, in case, for example, someone changes the configuration of the unit incorrectly. The **Configure** icon sends a saved file to the unit.*

ARP and Telnet

The unit’s IP address must be configured before a network connection is available. If the unit has no IP address, you can use the Address Resolution Protocol (ARP) method from UNIX and Windows-based systems to assign a temporary IP address. If you want to initially configure the unit through the network, follow these steps:

1. On a UNIX or Windows-based host, create an entry in the host's ARP table using the intended IP address and the hardware address of the unit, which is found on the product label on the bottom of the unit.

Figure 2-9. ARP on UNIX

```
arp -s 191.12.3.77 00:20:4a:xx:xx:xx
```

Note: *For the ARP command to work on Windows 95, the ARP table on the PC must have at least one IP address defined other than its own.*

2. If you are using Windows 95, type ARP -A at the DOS command prompt to verify that there is at least one entry in the ARP table. If the local machine is the only entry, ping another IP address on your network to build a new entry in the ARP table; the IP address must be a host other than the machine on which you are working. Once there is at least one additional entry in the ARP table, use the following command to ARP an IP address to the unit:

Figure 2-10. ARP on Windows

```
arp -s 191.12.3.77 00-20-4a-xx-xx-xx
```

3. Open a Telnet connection to port 1. The connection will fail quickly, but the unit will temporarily change its IP address to the one designated in this step.

Figure 2-11. Telnet to Port 1

```
telnet 191.12.3.77 1
```

4. Finally, open a Telnet connection to port 9999, and **press Enter within three seconds** to go into Setup Mode. If you wait longer than three seconds, the unit will reboot.

Figure 2-12. Telnet to Port 9999

```
telnet 191.12.3.77 9999
```

5. Set all required parameters

Note: *The IP address you just set is temporary and will revert to the default value when the unit 's power is reset unless you log into the unit and store the changes permanently. Refer to the chapter on configuration for instructions on permanently configuring the IP address.*

Serial Port Login

If you want to initially configure the unit through a serial connection, follow these steps:

1. Connect a console terminal or PC running a terminal emulation program to the unit's Channel 1 serial port. The default serial port settings are 9600 baud, 8 bits, no parity, 1 stop bit, no flow control.

2. To enter Setup Mode, cycle the unit's power (power off and back on). After power-up, the self-test begins and the red Diagnostic LED starts blinking. **You have one second** to enter three lowercase **x** characters.

   Note: *The easiest way to enter Setup Mode is to hold down the* ***x*** *key at the terminal (or emulation) while powering up the unit.*

3. Select **0** (Server Configuration) and follow the prompts until you get to IP address.
4. Enter the new IP address, Subnet Mask, and Gateway (if applicable).
5. Select **9** to save the configuration and exit Setup Mode. The unit performs a power reset.

3: Configuring the Unit

You must configure the unit so that it can communicate on a network with your serial device. For example, you must set the way the unit will respond to serial and network traffic, how it will handle serial packets, and when to start or close a connection. You can configure your unit locally or remotely using the following procedures:

- Use a standard Web browser to access the unit's internal Web pages and configure the unit over the network. This is the easiest and preferred method.
- Use a Telnet connection to configure the unit over the network.
- Use a terminal or terminal emulation program to access the serial port locally.

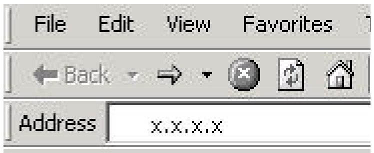
The unit's configuration is stored in nonvolatile memory (NVRam) and is retained without power. You can change the configuration at any time. The unit performs a reset after the configuration has been changed and stored.

Configuring via Web Browser

If your unit already has an IP address, you can log into it using a standard Web browser with Java enabled.

1. Type the unit's IP address into the Web browser's URL (Address/Location) field.

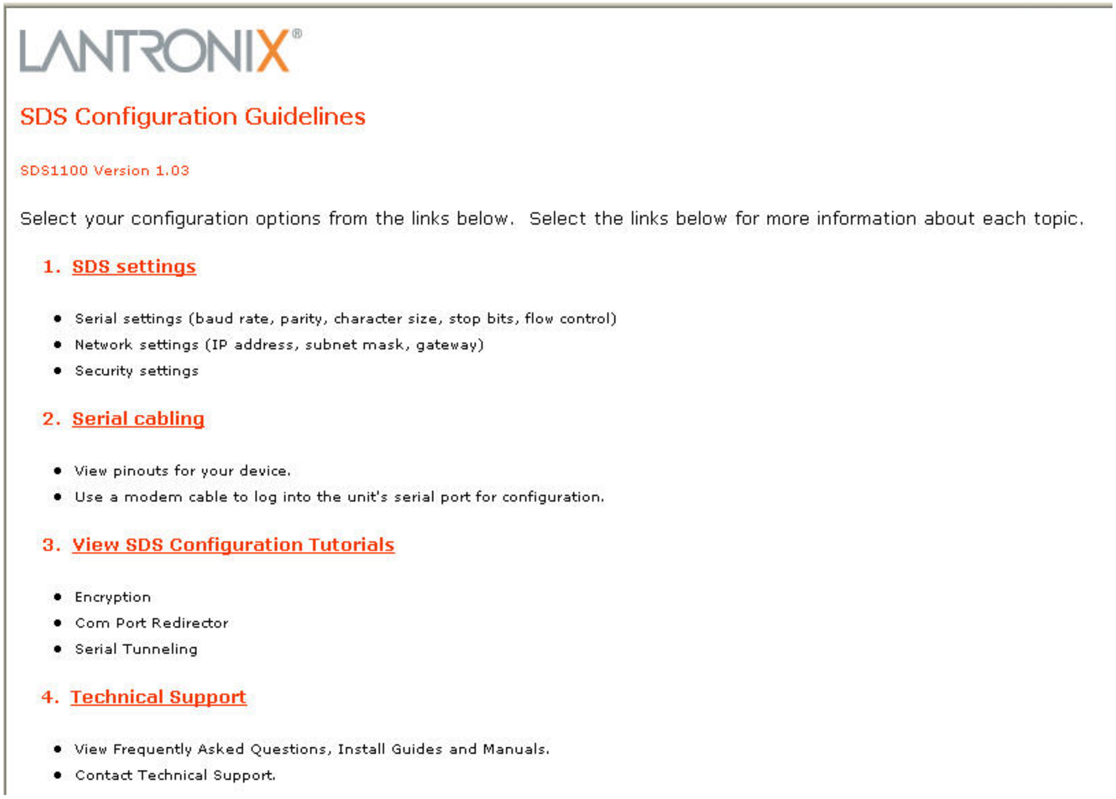
Figure 3-1. Web Browser Login



x.x.x.x

2. When the SDS Configuration Guidelines Page appears, select one of the four links:

Figure 3-2. SDS Configuration Guidelines Page



LANTRONIX®

SDS Configuration Guidelines

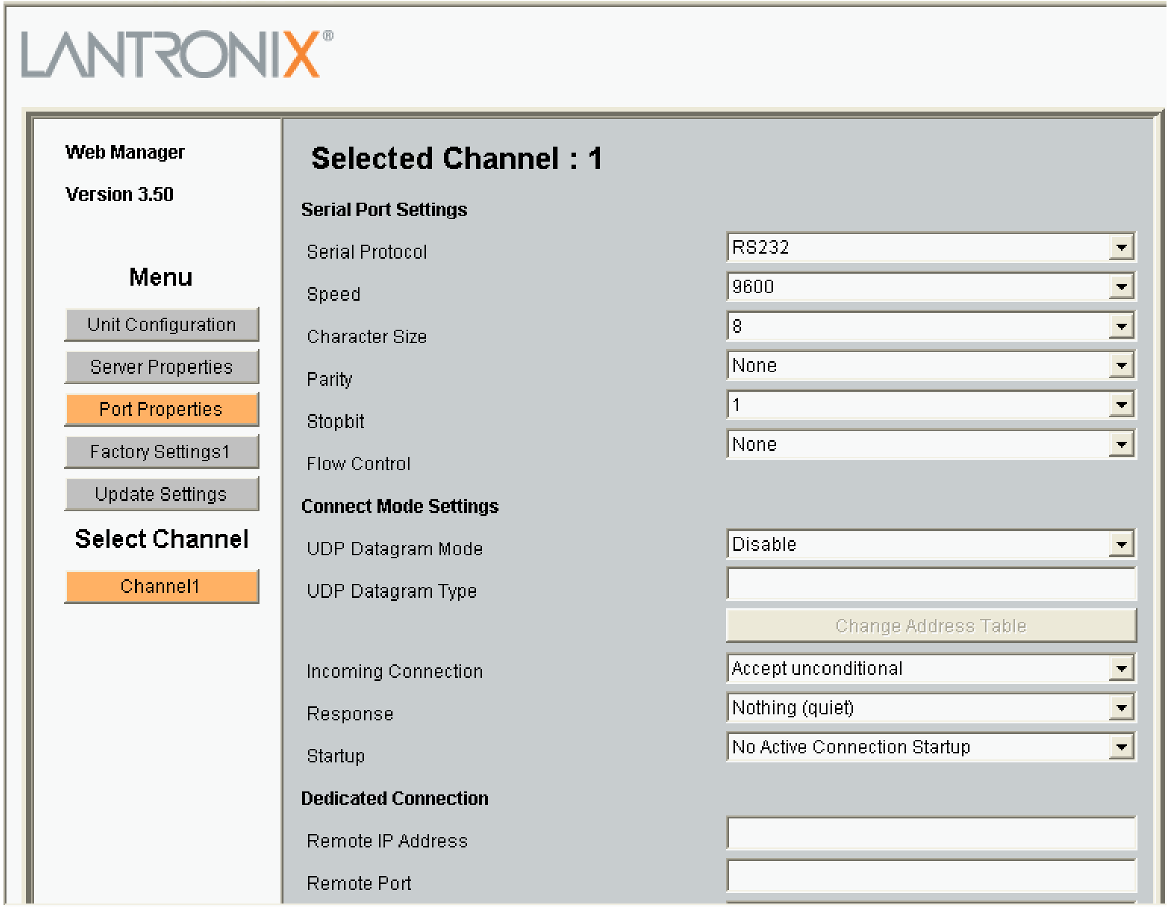
SDS1100 Version 1.03

Select your configuration options from the links below. Select the links below for more information about each topic.

1. SDS settings
   - Serial settings (baud rate, parity, character size, stop bits, flow control)
   - Network settings (IP address, subnet mask, gateway)
   - Security settings
2. Serial cabling
   - View pinouts for your device.
   - Use a modem cable to log into the unit's serial port for configuration.
3. View SDS Configuration Tutorials
   - Encryption
   - Com Port Redirector
   - Serial Tunneling
4. Technical Support
   - View Frequently Asked Questions, Install Guides and Manuals.
   - Contact Technical Support.

- **SDS settings** opens a configuration window to configure the SDS1100, as shown in Figure 3-3.
- **Serial cabling** lets you view pinouts for the SDS serial port.
- **View SDS Configuration Tutorials** provide step-by-step instructions for configuring encryption, serial tunneling, and the Com Port Redirector.
- **Technical Support** lets you download the latest firmware for your SDS and view documentation.

Figure 3-3. Lantronix WEB-Manager



Selected Channel : 1

Serial Port Settings	
Serial Protocol	RS232
Speed	9600
Character Size	8
Parity	None
Stopbit	1
Flow Control	None
Connect Mode Settings	
UDP Datagram Mode	Disable
UDP Datagram Type	
Incoming Connection	Accept unconditional
Response	Nothing (quiet)
Startup	No Active Connection Startup
Dedicated Connection	
Remote IP Address	
Remote Port	

To configure the unit via a Web browser, select **SDS Settings** and perform the following steps.

1. Use the menu (pushbuttons) to navigate to sub pages where you can configure server settings. See explanations of the configuration parameters later in this chapter.

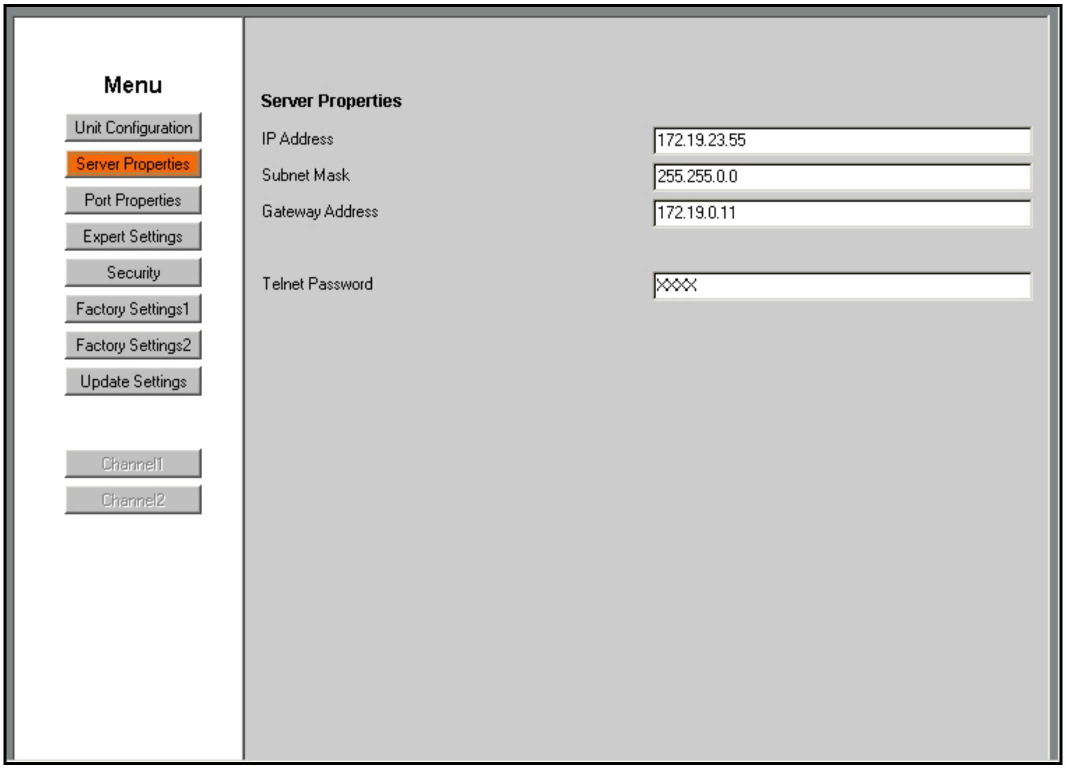
   Note: *The sequence of parameters explained and examples shown later in this chapter correspond to the Setup Mode window rather than to the WEB-Manager sub pages.*

2. When you are finished, click the **Update Settings** button to save your settings.

For example, to enter server properties:

1. Click the **Server Properties** button. The Server Properties section of the Web page displays.
2. Confirm or enter values for
   - IP Address
   - Subnet Mask
   - Gateway Address

Figure 3-4. Server Properties Configuration on the Web Browser



Server Properties

IP Address: 172.19.23.55

Subnet Mask: 255.255.0.0

Gateway Address: 172.19.0.11

Telnet Password: XXXX

3. In the **Telnet Password** field, enter a password to prevent unauthorized access to the Setup Mode via a Telnet connection to port 9999. The password is limited to 4 characters. (An enhanced password setting of 16 characters is available under *Security Settings* on the Telnet Setup Mode window.)

   Note: *No password is required to access the Setup Mode window via a serial connection.*

4. Click the **Update Settings** button.

Configuring via the Setup Mode Window

Using a Telnet Connection

To configure the unit over the network, establish a Telnet connection to port 9999.

Note: *You can also use the* ***Telnet to Device*** *icon on the DeviceInstaller Device Management window to establish the connection.*

1. From the Windows Start menu, click **Run** and type the following command, where x.x.x.x is the IP address and 9999 is the unit's fixed network configuration port number.

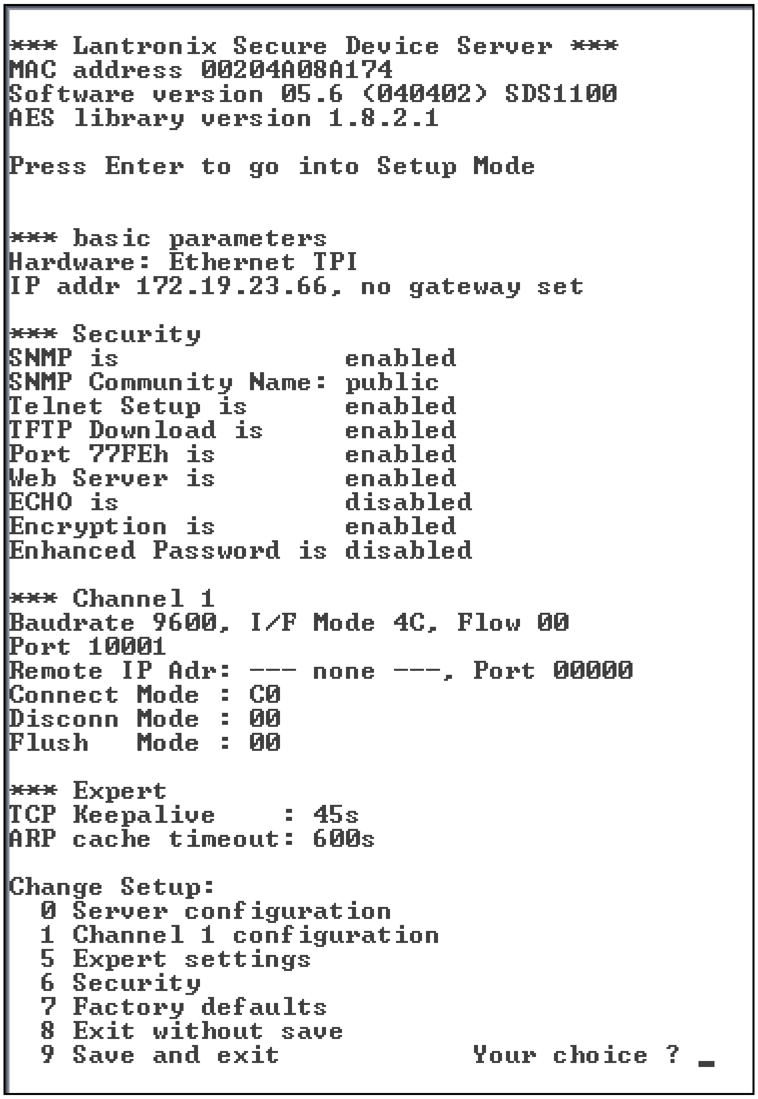
Figure 3-5. Network Login Using Telnet

```
telnet x.x.x.x 9999
```

Note: *Be sure to include a space between the IP address and 9999.*

2. Click **OK**. The Setup Mode window displays. To remain in Setup Mode, **you must press Enter within 5 seconds**.

Figure 3-6. Setup Mode Window



```
*** Lantronix Secure Device Server ***
MAC address 00204A08A174
Software version 05.6 (040402) SDS1100
AES library version 1.8.2.1

Press Enter to go into Setup Mode


*** basic parameters
Hardware: Ethernet TPI
IP addr 172.19.23.66, no gateway set

*** Security
SNMP is                 enabled
SNMP Community Name:    public
Telnet Setup is         enabled
TFTP Download is        enabled
Port 77FEh is           enabled
Web Server is           enabled
ECHO is                 disabled
Encryption is           enabled
Enhanced Password is disabled

*** Channel 1
Baudrate 9600, I/F Mode 4C, Flow 00
Port 10001
Remote IP Adr: --- none ---, Port 00000
Connect Mode : C0
Disconn Mode : 00
Flush   Mode : 00

*** Expert
TCP Keepalive    : 45s
ARP cache timeout: 600s

Change Setup:
  0 Server configuration
  1 Channel 1 configuration
  5 Expert settings
  6 Security
  7 Factory defaults
  8 Exit without save
  9 Save and exit            Your choice ? _
```

3. Select an option on the menu by entering the number of the option in the **Your choice ?** field and pressing **Enter.**

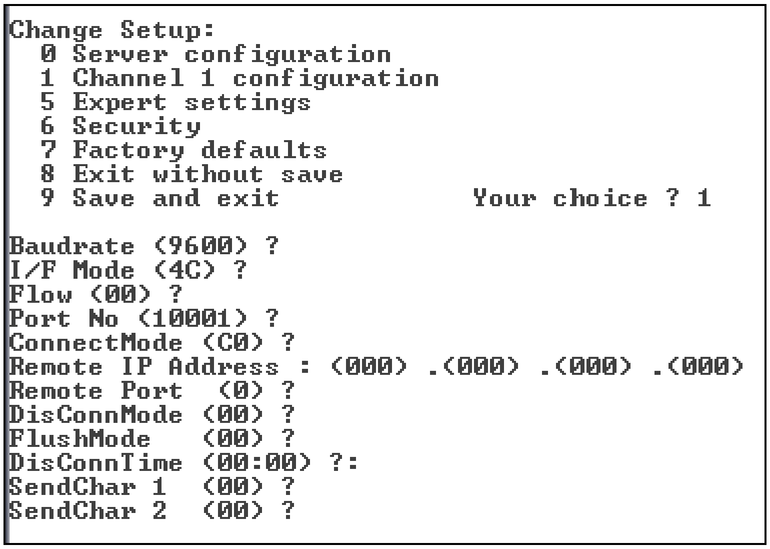
4. To enter a value for a parameter, type the value and press **Enter**, *or* to confirm a current value, just press **Enter**.

5. When you are finished, save the new configurations (option **9**). The unit will reboot.

For example, to set Channel 1 parameters:

1. Type **1** in the **Your choice?** field and press **Enter**.

Figure 3-7. Channel 1 Configuration



```
Change Setup:
  0 Server configuration
  1 Channel 1 configuration
  5 Expert settings
  6 Security
  7 Factory defaults
  8 Exit without save
  9 Save and exit            Your choice ? 1

Baudrate (9600) ?
I/F Mode (4C) ?
Flow (00) ?
Port No (10001) ?
ConnectMode (C0) ?
Remote IP Address : (000) .(000) .(000) .(000)
Remote Port  (0) ?
DisConnMode (00) ?
FlushMode   (00) ?
DisConnTime (00:00) ?:
SendChar 1  (00) ?
SendChar 2  (00) ?
```

2. In the **Baudrate** field, accept 9600 by pressing **Enter** or enter the speed you wish to use.

3. In the **I/F Mode** field accept the default (4C) or change the I/F (serial) settings.

4. Continue entering the listed parameters, or accept the defaults by pressing **Enter**:

5. When you are finished entering all of the parameters (all options), save the new configurations (option **9**). The unit will reboot.

Using the Serial Port

For local configuration, a terminal or a PC running a terminal emulation program can be connected to the unit's serial port (channel 1). The terminal (or emulation) should be configured for 9600 baud, 8-bit, no parity, 1 stop bit, and no flow control.

1. Cycle the unit's power (power off and back on). After power-up, the self-test begins and the diagnostic and status LEDs start blinking.

2. Type three lowercase **x** characters (**xxx**) **within one second** after powering up in order to start the configuration mode. The Setup Mode window displays. (See the example in *Using a Telnet Connection.)*

   Note: *The easiest way to enter Setup Mode is to hold down the* ***x*** *key on your keyboard while powering up the unit.*

3. Select an option on the menu by entering the number of the option in the **Your choice ?** field and pressing **Enter.**

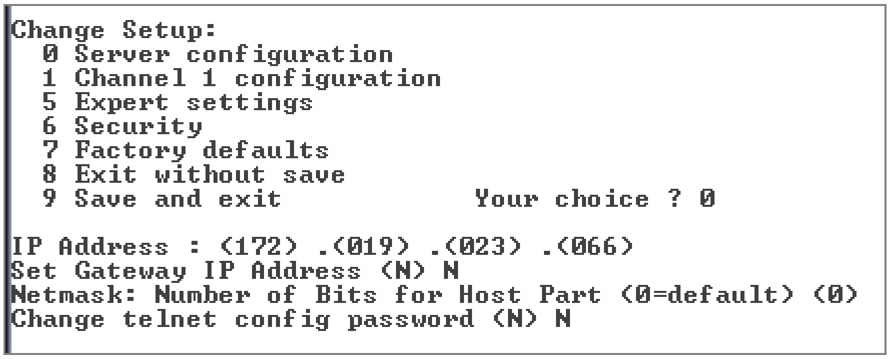
4. To enter a value for a parameter, type the value and press **Enter,** *or* to confirm a default value, just press **Enter**.

5. When you are finished, save the new configuration (option **9**). The unit will reboot.

Server Configuration (Network Configuration)

These are the unit's basic network parameters.

Figure 3-8. Network Configuration



```
Change Setup:
  0 Server configuration
  1 Channel 1 configuration
  5 Expert settings
  6 Security
  7 Factory defaults
  8 Exit without save
  9 Save and exit            Your choice ? 0

IP Address : (172) .(019) .(023) .(066)
Set Gateway IP Address (N) N
Netmask: Number of Bits for Host Part (0=default) (0)
Change telnet config password (N) N
```

IP Address

The IP address must be set to a unique value in your network. See Methods for Assigning the IP Address for more information about IP addressing.

Set Gateway IP Address

The gateway address, or router, allows communication to other LAN segments. The gateway address should be the IP address of the router connected to the same LAN segment as the unit. The gateway address must be within the local network.

Netmask

A netmask defines the number of bits taken from the IP address that are assigned for the host section.

Note: *Class A: 24 bits; Class B: 16 bits; Class C: 8 bits.*

The unit prompts for the number of host bits to be entered, then calculates the netmask, which is displayed in standard decimal-dot notation when the saved parameters are displayed (for example, 255.255.255.0).

Table 3-1. Standard IP Network Netmasks

Network Class	Host Bits	Netmask
A	24	255.0.0.0
B	16	255.255.0.0
C	8	255.255.255.0

Table 3-2. Netmask Examples

Netmask	Host Bits
255.255.255.252	2
255.255.255.248	3
255.255.255.240	4
255.255.255.224	5
255.255.255.192	6
255.255.255.128	7
255.255.255.0	8
255.255.254.0	9
255.255.252.0	10
255.255.248.0	11
...	...
255.128.0.0	23
255.0.0.0	24

Change Telnet configuration password

Setting the Telnet configuration password prevents unauthorized access of the setup menu via a Telnet connection to port 9999 or via Web pages. The password is limited to 4 characters. An enhanced password setting of 16 characters is available under Security Settings for Telnet access only.

Note: *No password is required to access the Setup Mode window via a serial connection.*

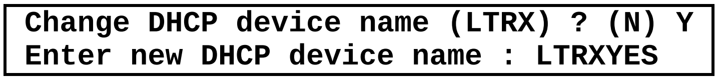
DHCP Naming

A DHCP name is a unique identifier used for managing multiple DHCP hosts on a network. Your unit ships with a default DHCP name of Cxxxxxx, where xxxxxx are the last six digits of the Mac address.

You can change the DHCP name (up to eight characters) when configuring the server on the Setup Mode window. Change the DHCP name to LTXdd, where 0.0.0.dd is the IP address assigned (dd should be a number between 1 and 99). For example, if the IP address is set to 0.0.0.5, the resulting DHCP name is LTX05. DHCP gives the unit a DHCP address when a LTX05 name is given.

If you give the unit an IP of 0.0.0.0, you then have the option to assign an 8-character DHCP name.

Figure 3-9. Server Configuration Option

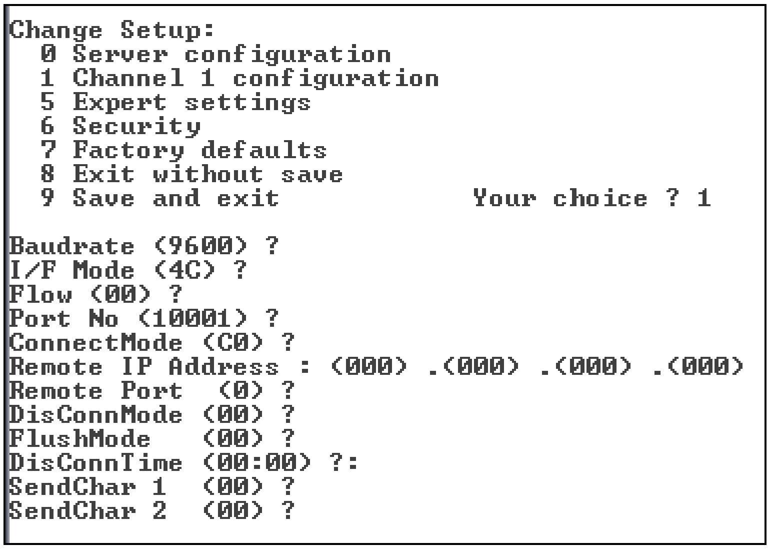


```
Change DHCP device name (LTRX) ? (N) Y
Enter new DHCP device name : LTRXYES
```

Channel 1 Configuration (Serial Port Parameters)

Using this option, define how the serial port will respond to network and serial communications.

Figure 3-10. Channel 1 Configuration



```
Change Setup:
  0 Server configuration
  1 Channel 1 configuration
  5 Expert settings
  6 Security
  7 Factory defaults
  8 Exit without save
  9 Save and exit            Your choice ? 1

Baudrate (9600) ?
I/F Mode (4C) ?
Flow (00) ?
Port No (10001) ?
ConnectMode (C0) ?
Remote IP Address : (000) .(000) .(000) .(000)
Remote Port   (0) ?
DisConnMode  (00) ?
FlushMode    (00) ?
DisConnTime  (00:00) ?:
SendChar 1   (00) ?
SendChar 2   (00) ?
```

Baudrate

The unit and attached serial device, such as a modem, must agree on a speed or baud rate to use for the serial connection. Valid baud rates are 300, 600, 1200, 2400, 4800, 9600 (default), 19200, 38400, 57600, and 115200 bits per second.

I/F (Interface) Mode

The Interface (I/F) Mode is a bit-coded byte that you enter in hexadecimal notation.

Note: If you do not want to convert the binary numbers to hexadecimals yourself, look up the values in Table 6-6. Interface Mode Options in the Binary to Hexadecimal chapter.

Table 3-3. Interface Mode Options

I/F Mode Option	Bit 7	6	5	4	3	2	1	0
RS-232C							0	0
RS-422/485							0	1
RS-485 2-wire							1	1
7 Bit					1	0		
8 Bit					1	1		
No Parity			0	0				
Even Parity			1	1				
Odd Parity			0	1				
1 Stop bit	0	1						
2 Stop bit	1	1						

The following table demonstrates how to build some common Interface Mode settings:

Table 3-4. Common Interface Mode Settings

Common I/F Mode Setting	Binary	Hex
RS-232C, 8-bit, No Parity, 1 stop bit	0100 1100	4C
RS-232C, 7-bit, Even Parity, 1 stop bit	0111 1000	78
RS-485 2-Wire, 8-bit, No Parity, 1 stop bit	0100 1111	4F
RS-422, 8-bit, Odd Parity, 1 stop bit	0101 1101	5D

Flow

Flow control sets the local handshake method for stopping serial input/output.

Table 3-5. Flow Control Options

Flow Control Option	Hex
No flow control	00
XON/XOFF flow control	01
Hardware handshake with RTS/CTS lines	02
XON/XOFF pass characters to host	05

Port Number

The setting represents the source port number in TCP connections. It is the number that identifies the channel for remote initiating connections. The default setting for Port 1 is 10001. The range is 1-65535, except for the following reserved port numbers:

Table 4-5. Reserved Port Numbers

Port Numbers	Reserved for
1 – 1024	Reserved (well known ports)
9999	Telnet setup
14000-14009	Reserved for Redirector
30718	Reserved (77FEh)

Warning:* *We recommend that you* not *use the reserved port numbers for this setting as incorrect operation may result.

The port number functions as the TCP/UDP source port number for outgoing packets. Packets sent to the unit with this port number are received to this channel. The port number selected is the Incoming TCP/UDP port and Outgoing TCP/UDP source port. Use Port 0 when you want the outgoing source port to change with each connection.

If the port number is 0, a random value of at least 50000 is used to actively establish a connection. Each subsequent connection increments the number by 1. When the port number reaches 59999, it wraps around to 50000.

Only use the automatic port increment feature to initiate a connection using TCP. Set the port to a non-zero value when the unit is in a passive mode or when you are using UDP instead of TCP.

Connect Mode

Connect Mode defines how the unit makes a connection, and how it reacts to incoming connections over the network. Enter Connect Mode options in hexadecimal notation.

Note: If you do not want to convert the binary numbers to hexadecimals yourself, look up the values in Table 6-2. Connect Mode Options in the Binary to Hexadecimal chapter.

Table 3-6. Connect Mode Options

Connect Mode Option	Bit 7	6	5	4	3	2	1	0
Incoming Connection								
Never accept incoming	0	0	0					
Accept incoming with DTR	0	1	0					
Accept unconditional	1	1	0					
Response								
Nothing (quiet)				0				
Character response (C=conn, D=disconn, N=unreachable)				1				
Startup								
No active startup					0	0	0	0
With any character					0	0	0	1
With active DTR					0	0	1	0
With a specific start character					0	0	1	1
Manual connection					0	1	0	0
Autostart					0	1	0	1
Hostlist	0	0	1	0				
Datagram Type								
Directed UDP					1	1	0	0
Modem Mode								
Full Verbose				1	0	1	1	0
Without Echo				0	0	1	1	0
Numeric modem result codes				1	0	1	1	1

Manual Connection: When you use manual connection, you are not required to enter the entire IP address if the IP is already configured as the remote IP address in the unit. For example, if the remote IP address already configured in the unit is 129.1.2.3, then an example command string would be C3/7. (This would connect to 129.1.2.3 and port 7.) You may also use a different ending for the connection string. For example, C50.1/23 would connect you to 129.1.50.1 and port 23.

Table 3-7. Manual Connection Address Example

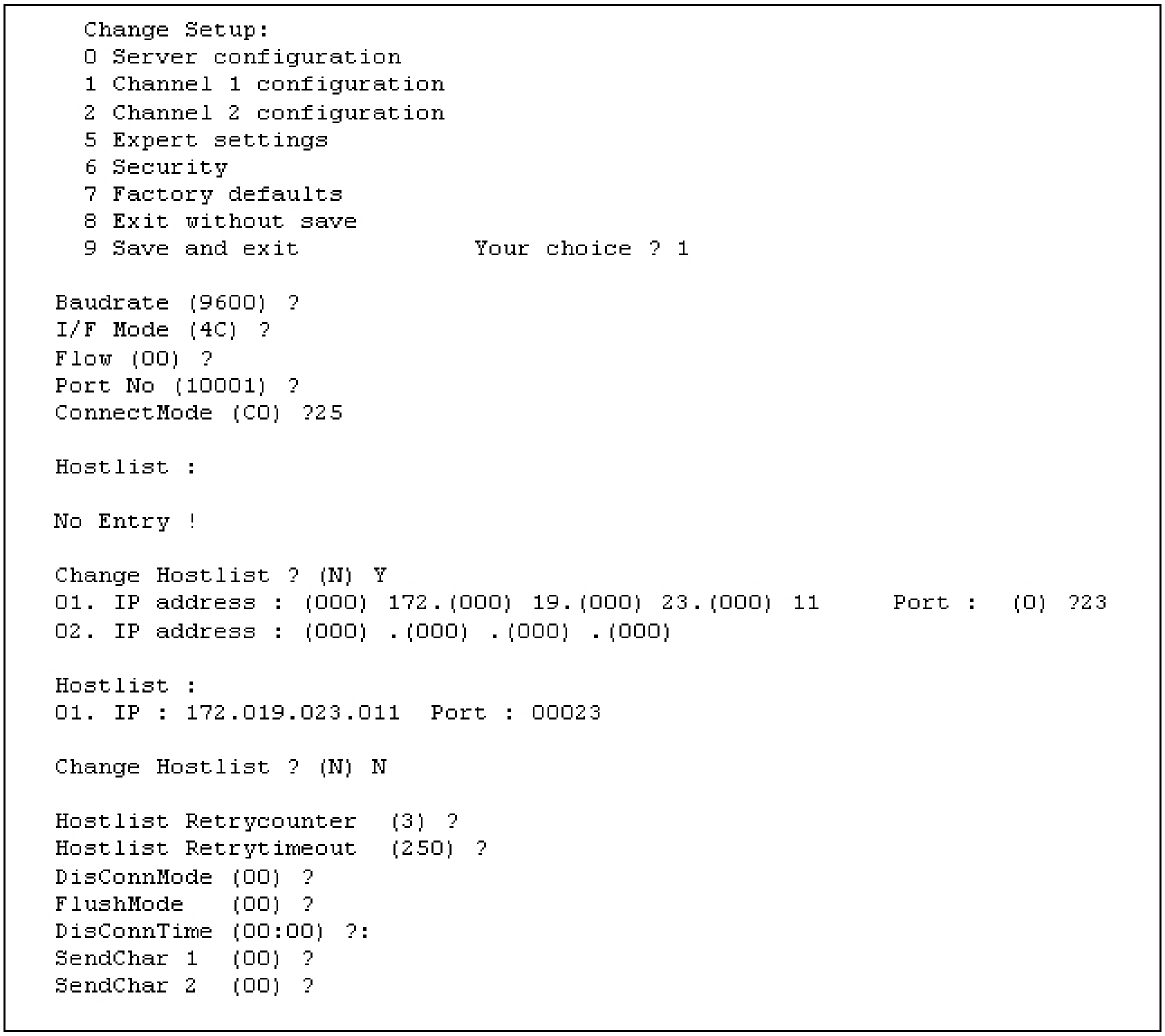
Command String	Result if remote IP is 129.1.2.3 and remote port is 1234
C121.2.4.5/1	Complete override; connection is started with host 121.2.4.5, port 1
C5	Connect to 129.1.2.5, port 1234
C28.10/12	Connect to 129.1.28.10, port 12

Autostart (Automatic Connection): If autostart is enabled, the unit automatically connects to the remote IP address and remote port specified.

Datagram Type: When selecting this option, you will be prompted for the Datagram type. Enter **01** for directed or broadcast UDP.

Hostlist: If you enable this option, the Lantronix unit scrolls through the hostlist until it connects to a device listed in the hostlist table. Once it connects, the unit stops trying to connect to any others. If this connection fails, the unit continues to scroll through the table until it is able to connect to another IP in the hostlist. Only Channel 1 supports the hostlist option.

Figure 3-11. Hostlist Option



```
  Change Setup:
  0 Server configuration
  1 Channel 1 configuration
  2 Channel 2 configuration
  5 Expert settings
  6 Security
  7 Factory defaults
  8 Exit without save
  9 Save and exit            Your choice ? 1

Baudrate (9600) ?
I/F Mode (4C) ?
Flow (00) ?
Port No (10001) ?
ConnectMode (C0) ?25

Hostlist :

No Entry !

Change Hostlist ? (N) Y
01. IP address : (000) 172.(000) 19.(000) 23.(000) 11      Port :  (0) ?23
02. IP address : (000) .(000) .(000) .(000)

Hostlist :
01. IP : 172.019.023.011  Port : 00023

Change Hostlist ? (N) N

Hostlist Retrycounter  (3) ?
Hostlist Retrytimeout  (250) ?
DisConnMode (00) ?
FlushMode   (00) ?
DisConnTime (00:00) ?:
SendChar 1  (00) ?
SendChar 2  (00) ?
```

To use this ability, follow these steps:

1. To enable the hostlist, enter a Connect Mode of 0x20 (**2X**). The menu shows you a list of current entries already defined in the product.
2. To delete, modify, or add an entry, select **Yes**. If you enter an IP address of 0.0.0.0, that entry and all others after it are deleted.
3. After completing the hostlist, repeat the previous step if necessary to edit the hostlist again.
4. For Retrycounter, enter the number of times the Lantronix unit should try to make a good network connection to a hostlist entry that it has successfully ARPed.
5. For Retrytimeout, enter the number of seconds the unit should wait before failing an attempted connection.

Modem (Emulation) Mode: In Modem Mode, the unit presents a modem interface to the attached serial device. It accepts AT-style modem commands, and handles the modem signals correctly.

Normally there is a modem connected to a local PC and a modem connected to a remote machine. A user must dial from the local PC to the remote machine, accumulating phone charges for each connection. Modem Mode allows you to replace modems with SDS1100s, and to use an Ethernet connection instead of a phone call, without having to change communications applications and make potentially expensive phone calls.

To select Modem Mode, set the Connect Mode to ***C6*** (no echo), ***D6*** (echo with full verbose), or **D7** (echo with 1-character response).

Note: *If the unit is in Modem Mode and the serial port is idle, the unit can still accept network TCP connections to the serial port if Connect Mode is set to **C6** (no echo), **D6** (echo with full verbose), or **D7** (echo with 1-character response).*

In Modem Mode, echo refers to the echo of all of the characters entered in command mode; it does not mean to echo data that is transferred. Quiet Mode (no echo) refers to the modem not sending an answer to the commands received (or displaying what was typed).

To disconnect a connection using Modem Mode commands:

- There must be 1-second guardtime (no data traffic) before sending +++.
- There must not be a break longer that 1 second between +s.
- There must be another 1-second guardtime after the last + is sent.
- The unit acknowledges with an **OK** to indicate that it is in command mode.
- Enter **ATH** and press **Enter**. It is echoed if echo is enabled. ATH is acknowledged by another **OK**.

Table 3-8. Modem Mode Commands

Modem Mode Command	Function
ATDTx.x.x.x,pppp or ATDTx.x.x.x/pppp	Makes a connection to an IP address (x.x.x.x) and a remote port number (pppp).
ATDTx.x.x.x	Makes a connection to an IP address (x.x.x.x) and the remote port number defined within the unit.
ATD0.0.0.0	Forces the unit into monitor mode if a remote IP address and port number are defined within the unit.
ATD	Forces the unit into monitor mode if a remote IP address and port number ***are not*** defined within the unit.
ATDx.x.x.x	Makes a connection to an IP address (x.x.x.x) and the remote port number defined within the unit.
ATH	Hangs up the connection (Entered as **+++ATH**).
ATDTx.x.x.x,pppp or ATDTx.x.x.x/pppp	Makes a connection to an IP address (x.x.x.x) and a remote port number (pppp).
ATS0=n	Enables or disables connections from the network going to the serial port. n=0 disables the ability to make a connection from the network to the serial port. n=1-9 enables the ability to make a connection from the network to the serial port. n>1-9 is invalid.
ATEn	Enables or disables character echo and responses. n=0 disables character echo and responses. n=1 enables character echo and responses.

ATVn	Enables 1-character response or full verbose.
	n=0 enables 1-character response.
	n=1 enables full verbose.

Note: *These AT commands are only recognized as single commands like ATE0 or ATV1; compound commands such as ATE0V1 are not recognized. All other AT commands with Modem Mode set to* full verbose *acknowledge with an OK, but no action is taken.*

Remote IP Address

This is the destination IP address used with an outgoing connection.

Remote Port

The remote TCP port number must be set for the unit to make outgoing connections. This parameter defines the port number on the target host to which a connection is attempted.

Note: *To connect an ASCII terminal to a host using the unit for login purposes, use the remote port number **23** (Internet standard port number for Telnet services).*

DisConnMode

In DisConnMode (Disconnect Mode), DSR drop either drops the connection or is ignored.

Note: If you do not want to convert the binary numbers to hexadecimals yourself, look up the values in *Table 6-4. Disconnect Mode Options* in the Binary to Hexadecimal chapter.

Table 3-9. Disconnect Mode Options

Disconnect Mode Option	Bit 7	6	5	4	3	2	1	0
Disconnect with DTR drop	1							
Ignore DTRa	0							
Telnet mode and terminal type setup[1]		1						
Channel (port) password[2]				1				
Hard disconnect[3]					0			
Disable hard disconnect					1			
State LED off with connection[4]								1
Disconnect with EOT (^D)[5]			1					

1. **The SDS will send the "Terminal Type" upon an outgoing connection.**
2. **A password is required for a connection to the serial port from the network.**
3. **The TCP connection will close even if the remote site does not acknowledge the disconnection.**
4. **When there is a network connection to or from the serial port, the state LED will turn off instead of blink.**
5. **When Ctrl D or Hex 04 are detected, the connection is dropped. Both Telnet mode and Disconnect with EOT must be enabled for Disconnect with EOT to function properly. Ctrl D will only be detected going from the serial port to the network.**

Flush Mode (Buffer Flushing)

Using this parameter, you can control line handling and network buffers with connection startup and disconnect. You can also select between two different packing algorithms.

Note: *If you do not want to convert the binary numbers to hexadecimals yourself, look up the values in Table 6-5. Flush Mode Options in the Binary to Hexadecimal chapter.*

Table 3-10. Flush Mode Options

Function	Bit 7	6	5	4	3	2	1	0
Input Buffer (Serial to Network)								
Clear with active connection (from serial)				1				
Clear with passive connection (from network)			1					
Clear with disconnect		1						
Output Buffer (Network to Serial)								
Clear with active connection (from serial)								1
Clear with passive connection (from network)							1	
Clear with disconnect						1		
Alternate Packing Algorithm (Pack Control)								
Enable	1							

Pack Control

Two firmware-selectable packing algorithms define how and when packets are sent to the network. The standard algorithm is optimized for applications in which the unit is used in a local environment, allowing for very small delays for single characters while keeping the packet count low. The alternate packing algorithm minimizes the packet count on the network and is especially useful in applications in a routed Wide Area Network (WAN). Adjusting parameters in this mode can economize the network data stream.

Pack control settings are enabled in Flush Mode. Set this value to **00** if specific functions are not needed.

Note: If you do not want to convert the binary numbers to hexadecimals yourself, look up the values in Table 6-7. Pack Control Options in the Binary to Hexadecimal chapter.

Table 3-11. Pack Control Options

Option	Bit 7	6	5	4	3	2	1	0
Idle Time								
Force transmit: 12ms							0	0
Force transmit: 52ms							0	1
Force transmit: 250ms							1	0
Force transmit: 5sec							1	1
Trailing Characters								
None					0	0		
One					0	1		
Two					1	0		
Send Characters								
2-Byte Send Character Sequence				1				
Send Immediately After Send chars			1					

Idle Time: Idle time to "Force transmit" defines how long the unit should wait before sending accumulated characters. This wait period is between characters. If there is an idle period between characters equal to the force transmit set, then the SDS will package up the serial data currently in the buffer and send it to the network.

Trailing Characters: In some applications, CRC, Checksum, or other trailing characters follow the end-of-sequence character; this option helps to adapt frame transmission to the frame boundary.

Send Characters: If 2-Byte Send Character Sequence is enabled, the unit interprets the sendchars as a 2-byte sequence; if not set, they are interpreted independently.

If Send Immediately After Send Characters is not set, any characters already in the serial buffer are included in the transmission after a "transmit" condition is found. If set, the unit sends immediately after recognizing the transmit condition (sendchar or timeout).

Note: A transmission might occur if status information needs to be exchanged or an acknowledgment needs to be sent.

DisConnTime (Inactivity Timeout)

Use this parameter to set an inactivity timeout. The connection is dropped if there is no activity on the serial line before the set time expires. Enter time in the following format: **mm:ss**, where **m** is the number of minutes and **s** is the number of seconds. To disable the inactivity timeout, enter **00:00**.

Send Characters

You can enter up to two characters in hexadecimal representation in the parameters "sendchar." If a character received on the serial line matches one of these characters, it is sent immediately, along with any awaiting characters, to the TCP connection. This minimizes the response time for specific protocol characters on the serial line (for example, ETX, EOT, etc.). Setting the first sendchar to **00** disables the recognition of the characters. Alternatively, the two characters can be interpreted as a sequence (see *Pack Control* above).

Telnet Terminal Type

This parameter appears only if the terminal type option is enabled in Disconnect Mode (see *DisConnMode* above). If this option is enabled, you can use the terminal name for the Telnet terminal type. Enter only one name.

If the terminal type option is enabled, the unit also reacts to the EOR (end of record) and binary options, which can be used for applications like terminal emulation to IBM hosts.

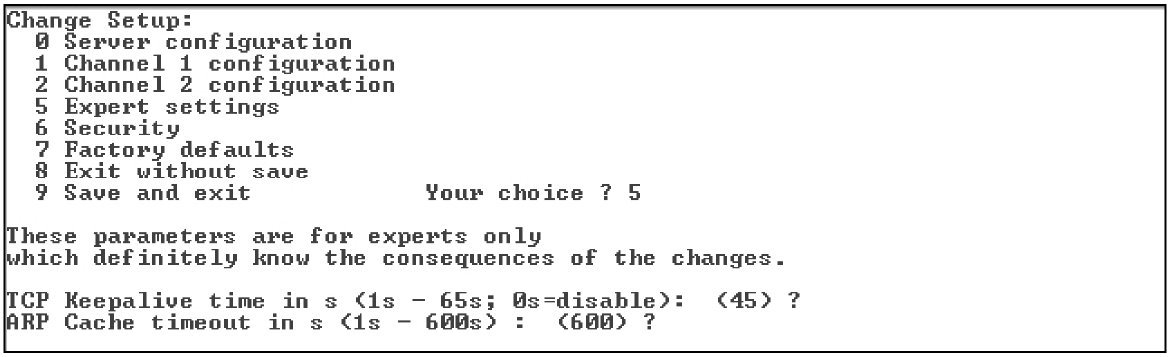
Channel (Port) Password

This parameter appears only if the channel (port) password option is enabled in Disconnect Mode (see above). If it is enabled, you can set a password on the serial port.

Expert Settings

Note: *You can change these settings via Telnet or serial connections only, not on the Web-Manager.*

Figure 3-12. Expert Settings Options



```
Change Setup:
  0 Server configuration
  1 Channel 1 configuration
  2 Channel 2 configuration
  5 Expert settings
  6 Security
  7 Factory defaults
  8 Exit without save
  9 Save and exit            Your choice ? 5

These parameters are for experts only
which definitely know the consequences of the changes.

TCP Keepalive time in s (1s - 65s; 0s=disable):  (45) ?
ARP Cache timeout in s (1s - 600s) :  (600) ?
```

TCP Keepalive time in s

This option allows you to change how many seconds the unit will wait during a silent connection before attempting to see if the currently connected network device is still on the network. If the unit then gets no response, it will drop that connection.

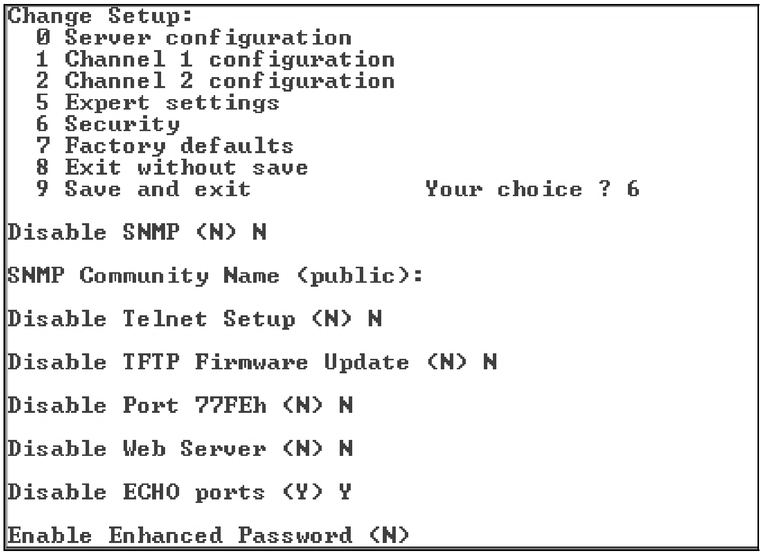
ARP Cache timeout in s

Whenever the unit communicates with another device on the network, it will add an entry into its ARP table. The ARP Cache timeout option allows you to define how many seconds (1-600) the unit will wait before timing out this table.

Security Settings

Note: *You can change these settings via Telnet or serial connections only, not on the Web-Manager. We recommend that you set security over the dedicated network or over the serial setup. If you set parameters over the network (Telnet 9999), someone else could capture these settings.*

Figure 3-13. Security Settings



```
Change Setup:
  0 Server configuration
  1 Channel 1 configuration
  2 Channel 2 configuration
  5 Expert settings
  6 Security
  7 Factory defaults
  8 Exit without save
  9 Save and exit            Your choice ? 6

Disable SNMP (N) N

SNMP Community Name (public):

Disable Telnet Setup (N) N

Disable TFTP Firmware Update (N) N

Disable Port 77FEh (N) N

Disable Web Server (N) N

Disable ECHO ports (Y) Y

Enable Enhanced Password (N)
```

Disable SNMP

This setting allows you to disable the SNMP protocol on the unit preventing SNMP management software from communicating with the SDS.

SNMP Community Name

This option allows you to change the SNMP Community Name on the unit. This allows for ease of management, and possibly some security. If someone tries to violate security but doesn’t know what community to connect to, that person will be unable to get the SNMP community information from the unit.

Disable Telnet Setup

This setting prevents remote access to this Configuration Menu by Telnet (port 9999). Remote configuration access will still be available using the web interface or locally via the serial port of the unit.

Disable TFTP Firmware Upgrade

This setting disables the use of TFTP to perform network firmware upgrades. With this option, firmware upgrades can be performed only by using a *.hex file over the serial port of the unit.

Disable Port 77FE (Hex)

Port 77FE is a setting that allows the Lantronix Device Installer utility to configure the unit remotely. Disabling Port 77FE will prevent remote access to the unit from the Lantronix Device Installer utility. You can configure the unit only by using Web pages, Telnet, or serial configuration.

Disable Web Setup

This setting disables the use of the Web Page Configuration tool that is built into the unit. Browser initiated sessions to port 80 on the SDS will be disabled. Configuration via HTTP will be disabled. Port 80 will be closed.

Enable Enhanced Password

This setting defaults to the N (option), which allows you to set a 4-character password that protects the Configuration Menu via Telnet and Web pages. The Y (Yes) option allows you to set an extended security password of 16-characters for protecting Telnet access.

Enable Encryption

Rijndael is the block cipher algorithm chosen by the National Institute of Science and Technology (NIST) as the Advanced Encryption Standard (AES) to be used by the US government. The SDS supports 128-, 192-, and 256-bit encryption key lengths.

Follow the steps below to configure AES encryption on the SDS.

NOTE: *Configuring encryption should be done through a local connection to the serial port of the SDS, or via a secured network connection. Initial configuration information including the encryption key are sent in clear text over the network.*

1. Telnet to the configuration port on the SDS (Port 9999).

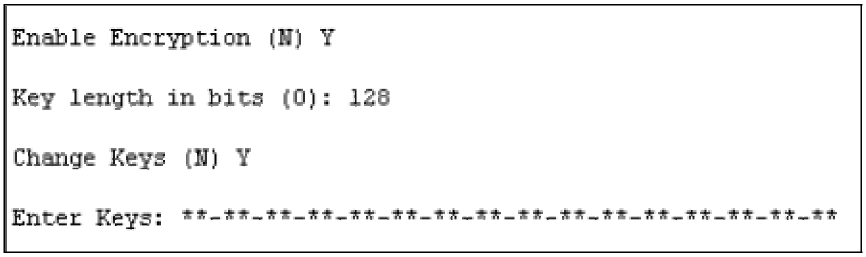
   An example of a Telnet command syntax is shown below. In the command examples below, replace the x's with the IP address of the SDS.

   Microsoft Windows command syntax: `xxx.xxx.xxx.xxx 9999`
   Unix command syntax: `xxx.xxx.xxx.xxx 9999`

2. When prompted, press **Enter** to go into setup mode.

3. At the Change Setup menu, select option **6** for security.

Figure 3-14. Encryption Keys



```
Enable Encryption (N) Y

Key length in bits (0): 128

Change Keys (N) Y

Enter Keys: **-**-**-**-**-**-**-**-**-**-**-**-**-**-**-**
```

4. When prompted to enable encryption, press **Y**.

5. Enter the encryption key length when prompted. The SDS supports 128-, 192-, and 256-bit encryption key lengths.

6. When prompted to change keys, press **Y**.

7. At the **Enter Keys** prompts, enter your encryption key. The encryption keys are entered in hexadecimal. The hexadecimal values are echoed as asterisks to prevent onlookers from seeing the key. Hexadecimal values are 0-9 and A-F.

   - For a 128-bit key length, enter 32 hexadecimal characters.
   - For a 192-bit key length, enter 48 hexadecimal characters.
   - For a 256-bit key length, enter 64 hexadecimal characters.

8. Continue pressing **Enter** until you return to the Change Setup menu.

9. At the Change Setup menu, select option **9** to save and exit.

Encryption only applies to the port selected for tunneling data (default 10001), regardless of whether you are using TCP or UDP.

Generally, one of two situations applies.

- Encrypted SDS-to-SDS communication. Be sure to configure both SDS devices with the same encryption key.
- Third-party application to SDS-encrypted communication: SDS uses standard AES encryption protocols. To communicate successfully, products and applications on the peer side must use the same protocols and the same shared key as the SDS. To ease the development process, Lantronix provides an AES encryption DLL for Windows and protocol source code samples. See the document "Encryption Enabling Serial Devices" on the Lantronix web site (www.lantronix.com) for more instructions and sample code.

Factory Default Settings

Select **7** to reset the unit's serial port to the factory default settings. The server configurations (IP address information) remain unchanged. The specific settings that this option changes appear in the following sections.

Channel 1 Configuration Defaults

Baudrate	9600
I/F Mode	4C (1 stop bit, no parity, 8 bit, RS-232C)
Own TCP port number	10001
Connect Mode	C0 (always accept incoming connection; no active connection startup)
Hostlist retry counter	3
Hostlist retry timeout	250 (msec)
Start character	0x0D (CR)
All other parameters	0

Expert Settings Defaults

TCP keepalive	45 (seconds)
ARP cache timeout	600 (seconds)

Security Settings Defaults

SNMP	Enabled
SNMP community name	public
Telnet setup	Enabled
TFTP download	Enabled
Port 77FEh	Enabled
Web Server	Enabled
ECHO	Disabled
Encryption	Disabled
Enhanced password	Disabled

Exit Configuration Mode

Select **8** to exit the configuration mode without saving any changes or rebooting, *OR* select **9** to reboot and save all changes. All values are stored in nonvolatile memory.

4: Updating Firmware

Obtaining Firmware

You can obtain the most up-to-date firmware and release notes for the unit from the Lantronix Web site (www.lantronix.com) or by using anonymous FTP (ftp://ftp.lantronix.com/).

Reloading Firmware

There are several ways to update the unit's internal operational code (**SD11*.ROM** or **SD11*.HEX**): via DeviceInstaller (the preferred way), via TFTP, via another unit, or via serial port. You can also update the unit's internal Web interface (**CBXW*.COB**) via TFTP or DeviceInstaller.

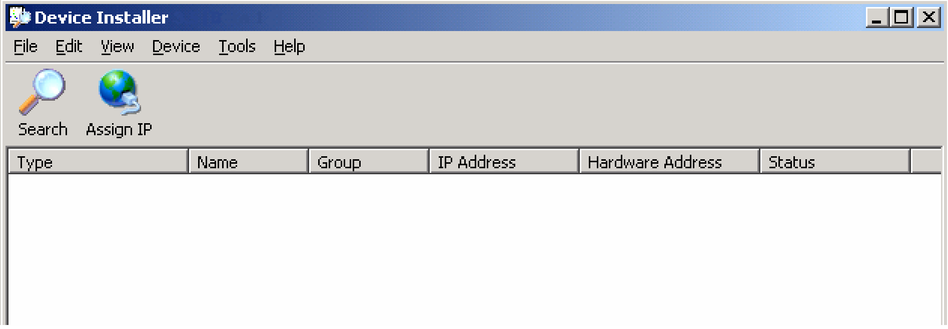
Via DeviceInstaller

After downloading the firmware to your computer, you can use DeviceInstaller to install it. If you haven't already installed DeviceInstaller from the product CD, see *Install the DeviceInstaller*.

1. Download the updated firmware files from www.lantronix.com or ftp://ftp.lantronix.com/ and store them in a subfolder on your computer.

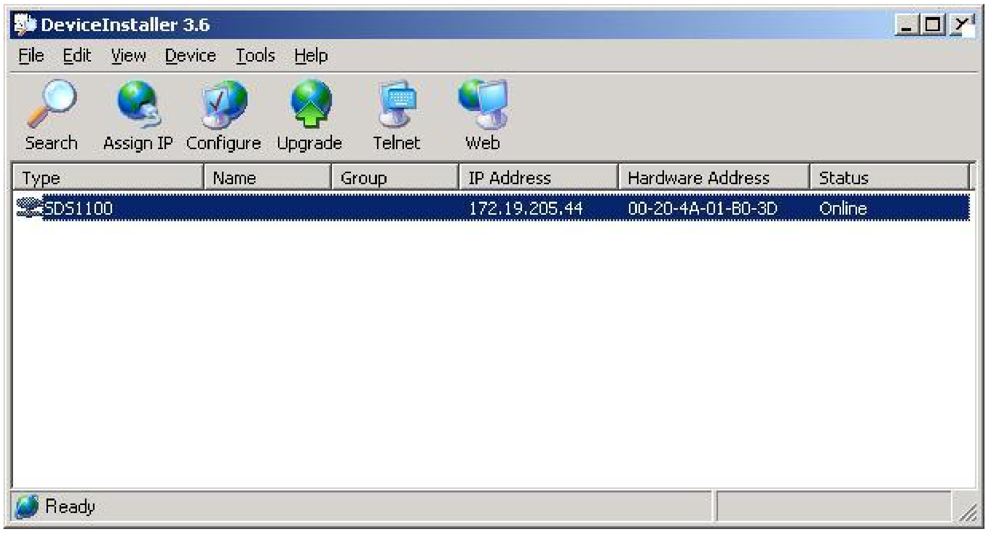
2. Click the **Start** button on the Task Bar and select **Programs → Lantronix → DeviceInstaller → Device Installer**. The DeviceInstaller window displays.

Figure 4-1. DeviceInstaller Window



3. Click the **Search the network for devices** icon. Search The Search Network window displays.

Figure 4-2. Search Network Window



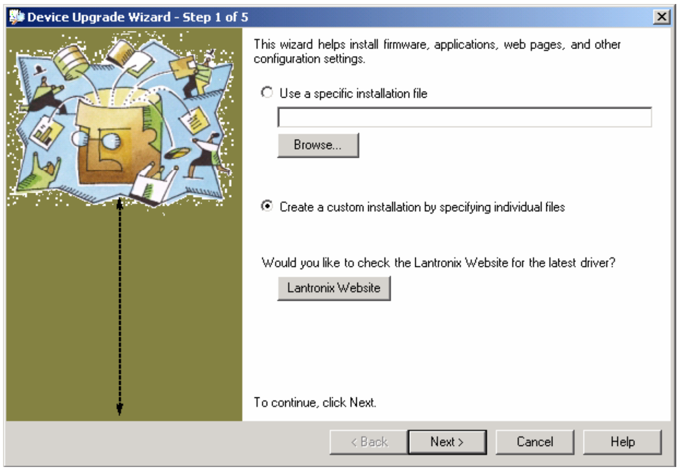
Type	Name	Group	IP Address	Hardware Address	Status
SDS1100			172.19.205.44	00-20-4A-01-B0-3D	Online

Ready

4. Once located by DeviceInstaller, highlight the device in the device list and click the **Upgrade** button.

5. Select a custom installation by specifying the individual files and clicking **Next**.

Figure 4-3. Device Upgrade Wizard (Step 1)



This wizard helps install firmware, applications, web pages, and other configuration settings.

○ Use a specific installation file

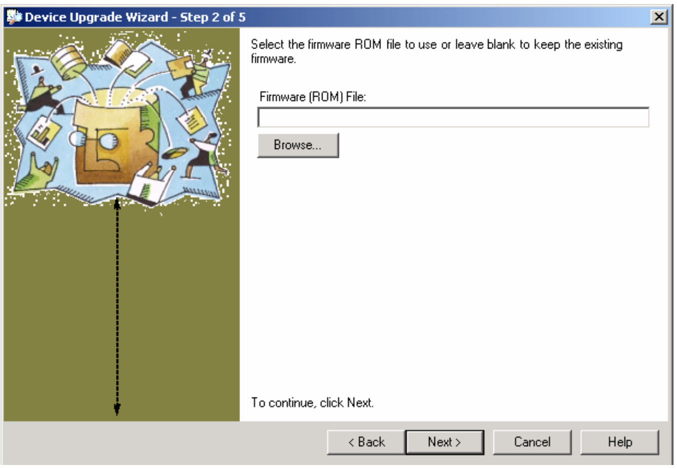
● Create a custom installation by specifying individual files

Would you like to check the Lantronix Website for the latest driver?

To continue, click Next.

6. Click the **Browse** button to select the location of the firmware file being loaded, then click **Next**.

Figure 4-4. Device Upgrade Wizard (Step 2)



Select the firmware ROM file to use or leave blank to keep the existing firmware.

Firmware (ROM) File:

To continue, click Next.

7. Select **Do not copy or replace any files** and click **Next**.

8. Click **Next** again. The status of the upgrade is shown in the window.

9. After the upgrade completes, click **Close**.

Via TFTP

Note: *If you are running Windows NT or later, you can simply enter the following command at the command prompt:*

TFTP –i IP address of SDS PUT source file name destination file name

It is easiest to issue the command from the same directory as the one where the firmware files are located.

To download new firmware using a TFTP client:

1. Use a TFTP client to send a binary file (**SD11*.ROM**) to the unit to upgrade the unit's internal operational code, and **cbx***.cob** to upgrade its internal Web interface).

   Note: *TFTP requires the **.ROM** (binary) version of the unit's internal operational code.*

2. Make sure the **Put** and **Binary** options at the top of the window are selected.

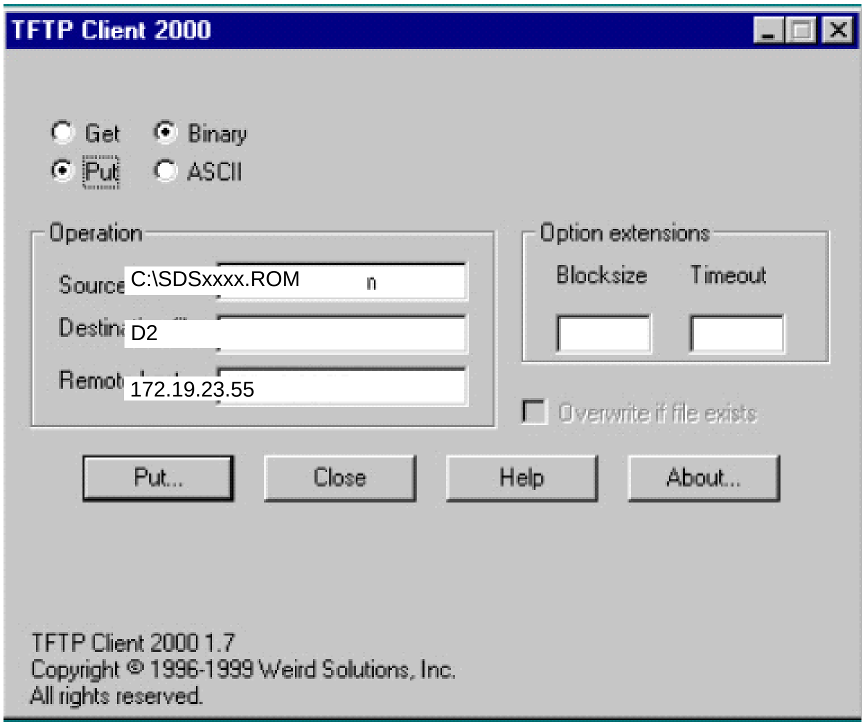
3. Enter the full path of the firmware file in the **Source File** field.

4. In the **Destination File** field, type **D1** for the internal operational code, or **WEB6** for the internal Web interface.

5. In the **Remote Host** field, enter the IP address of the unit being upgraded.

6. Click the **Put** button to transfer the file to the unit.

Figure 4-5. TFTP Dialog Box



TFTP Client 2000

○ Get ● Binary

● Put ○ ASCII

Operation

Source C:\SDSxxxx.ROM

Destin D2

Remot 172.19.23.55

Option extensions

Blocksize

Timeout

□ Overwrite if file exists

TFTP Client 2000 1.7
Copyright © 1996-1999 Weird Solutions, Inc.
All rights reserved.

The unit performs a power reset after the firmware has been loaded and stored.

Via Another Unit

To distribute firmware to another unit over the network:

1. Enter the host unit's Monitor Mode (see *Monitor Mode* in the Troubleshooting chapter).
2. Send the firmware to the receiving unit using the **SF** command, where x.x.x.x is the receiving unit's IP address.

Figure 4-6. Sending Firmware to Another Unit

```
SF x.x.x.x
```

The receiving unit performs a power reset after the firmware has been loaded and stored.

Note: *You can only update your unit 's internal Web interface using TFTP or DeviceInstaller.*

Via the Serial Port

The following procedure is for using the HyperTerminal software application. This procedure takes about 10 minutes.

Note: ***Do not switch off the power supply during the update****. A loss of power while reprogramming will result in a corrupt program image and a nonfunctional unit.*

To download firmware from a computer via the unit's serial port:

1. Enter Monitor Mode via the serial port. (see *Monitor Mode* in the Troubleshooting chapter).
2. Download the firmware to the unit using the **DL** command.
3. Select **Send Text File** and select the **SD11*.HEX** file to be downloaded. The downloaded file must be the **.HEX** (ASCII) version.
4. After the final record is received, the unit checks the integrity of the firmware image before programming the new firmware in the flash ROM. The following message displays when the firmware upgrade is complete.

Figure 4-7. Firmware Upgrade Screen Display

```
*** NodeSet 2.0 ***
0>DL
02049 lines loaded.
```

Note: You can only update your unit 's internal Web interface using TFTP or DeviceInstaller.

5: Troubleshooting

This chapter discusses how you can diagnose and fix errors quickly without having to contact a dealer or Lantronix.

It helps to connect a terminal to the serial port while diagnosing an error to view summary messages that may be displayed. When troubleshooting, always ensure that the physical connections (power cable, network cable, and serial cable) are secure.

Note: Some unexplained errors might be caused by duplicate IP addresses on the network. Make sure that your unit's IP address is unique.

Technical Support

If you are experiencing an error that is not described in this chapter, or if you are unable to fix the error, you may:

- Check our online knowledge base at www.lantronix.com/support.com
- E-mail us at support@lantronix.com
- Call us at:

  (800) 422-7044 Domestic

  (949) 453-7198 International

  (949) 450-7226 Fax

Our phone lines are open from 6:00AM - 5:30 PM Pacific Time Monday through Friday excluding holidays.

Technical Support Europe, Middle East, and Africa
Phone: +49 (0) 7720 3016 57
Fax: +49(0) 7720 3016 88
E-mail: eu_techsupp@lantronix.com

Firmware downloads, FAQs, and the most up-to-date documentation are available at: www.lantronix.com/support

When you report a problem, please provide the following information:

- Your name, and your company name, address, and phone number
- Lantronix SDS model number
- Lantronix SDS serial number
- Software version (on the first screen shown when you Telnet to port 9999)
- Description of the problem
- Debug report (stack dump), if applicable
- Status of the unit when the problem occurred (please try to include information on user and network activity at the time of the problem)

Table 5-1. Problems and Error Messages

Note: *When troubleshooting the following problems, make sure that the SDS is powered up and the Link LED is lit solid green. If the Link LED is not lit, then the physical network connection is bad. Confirm that you are using a good network connection.*

Problem/Message	Reason	Solution
When you issue the ARP –S command in Windows, “The ARP entry addition failed: 5" message displays.	Your currently logged-in user does not have the correct rights to use this command on this PC.	Have someone from your IT department log you in with sufficient rights.
When you attempted to assign an IP address to the SDS via the ARP method, the “Press Enter to go into Setup Mode” error (described below) displayed. Now when you Telnet to the SDS, the connection fails.	When you Telnet into port 1 on the SDS, you are only assigning a temporary IP address. When you Telnet into port 9999 and do not press Enter quickly, the SDS will reboot, causing it to lose the IP address.	Telnet back into Port 1. Wait for it to fail, then Telnet to port 9999 again. Make sure you press Enter quickly.
When you Telnet to port 9999, the message “Press Enter to go into Setup Mode*”* displays. However, nothing happens when you press Enter, or your connection is closed.	You did not press Enter quickly enough. You only have 5 seconds to press Enter before the connection is closed.	Telnet to port 9999 again, but press Enter as soon as you see the message “Press Enter to go into Setup Mode.”
When you Telnet to port 1 to assign an IP address to the SDS, the Telnet window does not respond for a long time.	You may have entered the Ethernet address incorrectly with the ARP command.	Confirm that the Ethernet address that you entered with the ARP command is correct. The Ethernet address may only include numbers 0-9 and letters A-F. In Windows and usually in Unix, the segments of the Ethernet address are separated by dashes. In some forms of Unix, the Ethernet address is segmented with colons.

Problem/Message	Reason	Solution
	The IP address you are trying to assign is not on your logical subnet.	Confirm that your PC has an IP address and that it is in the same logical subnet that you are trying to assign to the SDS.
	The SDS may not be plugged into the network properly.	Make sure that the Link LED is lit. If the Link LED is not lit, then the SDS is not properly plugged into the network.
When you try to assign an IP with DeviceInstaller, you get the following message: "No response from device! Verify the IP, Hardware address and Network Class. Please try again."	The cause is most likely one of the following: The Hardware address you specified is incorrect. The IP address you are trying to assign is not a valid IP for your logical subnet. You did not choose the correct subnet mask.	Double-check the parameters that you specified. Tip: You cannot assign an IP address to a SDS through a router.
No LEDs are lit.	The unit or its power supply is damaged, or the unit is not plugged into power properly.	Try plugging the SDS into another outlet. If this does not fix the problem, contact your dealer or Lantronix Technical Support for a replacement.
The SDS1100 will not power up properly, and the LEDs are flashing.	Various	Consult the LEDs section in the Introduction chapter or the Quick Start for the LED flashing sequence patterns. Call Lantronix Technical Support if the blinking pattern indicates a critical error.
The SDS is not communicating with the serial device attached to the SDS.	The most likely reason is the wrong serial cable or serial settings were chosen.	Make sure that you are using the correct serial cable. The SDS serial port is just like a modem serial port (DCE). The serial settings for the serial device and the SDS must match. The default serial settings for the SDS are RS232, 9600 Baud, 8 Character Bits, No Parity, 1 Stop Bit, No Flow Control.
When you try to enter the setup mode on the SDS via the serial cable, you get no response.	The issue will most likely be something covered in the previous problem, or possibly you have Caps Lock on.	Double-check everything in the problem above. Confirm that Caps Lock is not on.

Problem/Message	Reason	Solution
You can ping the SDS, but not Telnet to the SDS on port 9999.	There may be an IP address conflict on your network. You are not Telneting to port 9999. The Telnet configuration port (9999) is disabled within the SDS security settings. The unit may have the correct IP address, but an incorrect gateway address.	Turn the SDS off and then issue the following commands at the DOS prompt of your computer: ARP -D X.X.X.X (X.X.X.X is the IP of the SDS) PING X.X.X.X (X.X.X.X is the IP of the SDS). If you get a response, then there is a duplicate IP address on the network (the LEDs on the SDS should flash a sequence that tells you this). If you do not get a response, use the serial port to verify that Telnet is not disabled.
With DeviceInstaller you get the “Wrong Password” error when you try to upgrade the firmware.	You have chosen the incorrect setting for the Existing Firmware filed.	Try upgrading the firmware again, but make sure to use the correct setting in the field of Existing Firmware field.
You are using the correct serial cable, and the SDS should be set up correctly, but you are not communicating with your device attached to the SDS across the network.	If you are sure that the serial cable is correct, then you may not be connecting to the correct socket of the SDS. Another possibility is that the SDS is not set up correctly to make a good socket connection to the network.	You can check to see whether there is a socket connection to or from the SDS by looking at the Status LED. If the Status LED is blinking consistently, or is completely off, then there is a good socket connection. If the Status LED is solid green, then the socket connection does not exist. Use the Connect Mode option C0 for making a connection to the SDS from the network. Use Connect Mode option C1 or C5 for a connection to the network from the SDS. See the full list of *Connect Mode Options* in the Binary to Hexadecimal chapter.
When connecting to the Web-Manager within the SDS, the message “No Connection With The SDS” displays.	Your computer is not able to connect to port 30718 (77FEh) on the SDS.	Make sure that port 30718 (77FEh) is not blocked with any router that you are using on the network. Also make sure that port 77FEh is not disabled within the Security settings of the SDS.

Monitor Mode

Monitor Mode is a command-line interface used for diagnostic purposes (see *Monitor Mode Commands* at the end of this section). There are two ways to enter Monitor Mode: locally via the serial port or remotely via the network.

Via the Serial Port

To enter Monitor Mode locally, follow the same principles used in setting the serial configuration parameters:

1. To enter Monitor Mode with network connections, type **xx1** or **zzz** (not three x keys as you did before).

   OR

2. To enter Monitor Mode without network connections, type **xx2** or **yyy**.

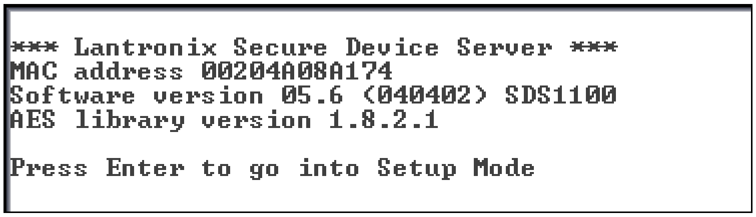
A **0>** prompt indicates that you have successfully entered Monitor Mode.

Via the Network

To enter Monitor Mode using a Telnet connection:

1. First establish a Telnet session. The following message displays:

Figure 5-1. Entering Monitor Mode Via the Network



```
*** Lantronix Secure Device Server ***
MAC address 00204A08A174
Software version 05.6 (040402) SDS1100
AES library version 1.8.2.1

Press Enter to go into Setup Mode
```

2. Type **M** (upper case).

A **0>** prompt indicates that you have successfully entered Monitor Mode.

Monitor Mode Commands

The following commands are available in Monitor Mode. Many commands have an IP address as an optional parameter (x.x.x.x). If the IP address is given, the command is applied to another unit with that IP address. If no IP address is given, the command is executed locally.

Note: *All commands must be given in capital letters, with blank spaces between the parameters.*

Table 5-2. Monitor Mode Commands

Command	Command Name	Function
SF x.x.x.x	Send Firmware	Sends firmware to unit with IP address x.x.x.x
VS x.x.x.x	Version	Queries software header record (16-byte) of unit with IP address x.x.x.x
GC x.x.x.x	Get Configuration	Gets configuration of unit with IP address x.x.x.x as hex records
SC x.x.x.x	Send Configuration	Sets configuration of unit with IP address x.x.x.x from hex records
PI x.x.x.x	Ping	Pings unit with IP address x.x.x.x to check device status
AT	ARP Table	Shows the unit 's ARP table entries
TT	TCP Connection Table	Shows all incoming and outgoing TCP connections
NC	Network Connection	Shows the unit 's IP configuration
RS	Reset	Resets the unit 's power
QU	Quit	Exits diagnostics mode
G0, G1...GE, GF	Get configuration from memory page	Gets a memory page of configuration information from the device.
S0, S1... SE, SF	Set configuration to memory page	Sets a memory page of configuration information on the device.

Entering any of the commands listed above will generate one of the following command response codes:

Table 5-3. Command Response Codes

Response	Meaning
0>	OK; no error
1>	No answer from remote device
2>	Cannot reach remote device or no answer
8>	Wrong parameter(s)
9>	Invalid command

6: Binary to Hexadecimal

Many of the unit 's configuration procedures require you to assemble a series of options (represented as bits) into a complete command (represented as a byte). The resulting binary value must be converted to a hexadecimal representation.

Use this chapter to learn how to convert binary values to hexadecimals or to look up values in the tables listing all configuration options in hexadecimal notation. The following tables are included:

- Binary to Hexadecimal Conversions
- Connect Mode Options
- Disconnect Mode Options
- Flush Mode (Buffer Flushing) Options
- Interface Mode Options
- Pack Control Options

Converting Binary to Hexadecimal

Hexadecimal digits have values ranging from 0 to F, which are represented as 0-9, A (for 10), B (for 11), etc. To convert a binary value (for example, 0010 0011) to a hexadecimal representation, the upper and lower four bits are treated separately, resulting in a two-digit hexadecimal number (in this case, 4C). Use the following table to convert values from binary to hexadecimal.

Table 6-1. Binary to Hexadecimal Conversions

Decimal	Binary	Hex
0	0000	0
1	0001	1
2	0010	2
3	0011	3
4	0100	4
5	0101	5
6	0110	6
7	0111	7
8	1000	8
9	1001	9
10	1010	A
11	1011	B
12	1100	C
13	1101	D
14	1110	E
15	1111	F

Connect Mode Options

Note: *Character response codes are C=conn, D=disconn, N=unreachable*

Table 6-2. Connect Mode Options

Accept Incoming Connections	Serial Response Upon Connection	Active Connection Startup	Hostlist	Hex
Never	None (quiet)	No active startup		N/A
Never	None (quiet)	Any character		1
Never	None (quiet)	Active DTR		2
Never	None (quiet)	CR (0x0D)		3
Never	None (quiet)	Manual connection		4
Never	None (quiet)	Autostart		5
Never	None (quiet)	UDP		C
Never	Character	No active startup		10
Never	Character	Any character		11
Never	Character	Active DTR		12
Never	Character	CR (0x0D)		13
Never	Character	Manual connection		14
Never	Character	Autostart		15
Never	Character	UDP		1C
With DTR	None (quiet)	No active startup		40
With DTR	None (quiet)	Any character		41
With DTR	None (quiet)	Active DTR		42
With DTR	None (quiet)	CR (0x0D)		43

Accept Incoming Connections	Serial Response Upon Connection	Active Connection Startup	Hostlist	Hex
With DTR	None (quiet)	Manual connection		44
With DTR	None (quiet)	Autostart		45
With DTR	None (quiet)	UDP		4C
With DTR	Character	No active startup		50
With DTR	Character	Any character		51
With DTR	Character	Active DTR		52
With DTR	Character	CR (0x0D)		53
With DTR	Character	Manual connection		54
With DTR	Character	Autostart		55
With DTR	Character	UDP		N/A
Unconditionally	None (quiet)	No active startup		C0
Unconditionally	None (quiet)	Any character		C1
Unconditionally	None (quiet)	Active DTR		C2
Unconditionally	None (quiet)	CR (0x0D)		C3
Unconditionally	None (quiet)	Manual connection		C4
Unconditionally	None (quiet)	Autostart		C5
Unconditionally	None (quiet)	UDP		CC
Unconditionally	Character	No active startup		D0
Unconditionally	Character	Any character		D1
Unconditionally	Character	Active DTR		D2
Unconditionally	Character	CR (0x0D)		D3
Unconditionally	Character	Manual connection		D4
Unconditionally	Character	Autostart		D5
Unconditionally	Character	UDP		DC
Never	None (quiet)	No active startup	Hostlist	N/A
Never	None (quiet)	Any character	Hostlist	21
Never	None (quiet)	Active DTR	Hostlist	22
Never	None (quiet)	CR (0x0D)	Hostlist	23
Never	None (quiet)	Manual connection	Hostlist	N/A
Never	None (quiet)	Autostart	Hostlist	25
Never	None (quiet)	UDP	Hostlist	N/A
Never	Character	No active startup	Hostlist	N/A
Never	Character	Any character	Hostlist	31
Never	Character	Active DTR	Hostlist	32
Never	Character	CR (0x0D)	Hostlist	33
Never	Character	Manual connection	Hostlist	N/A
Never	Character	Autostart	Hostlist	35
Never	Character	UDP	Hostlist	N/A

Accept Incoming Connections	Serial Response Upon Connection	Active Connection Startup	Hostlist	Hex
With DTR	None (quiet)	No active startup	Hostlist	N/A
With DTR	None (quiet)	Any character	Hostlist	61
With DTR	None (quiet)	Active DTR	Hostlist	62
With DTR	None (quiet)	CR (0x0D)	Hostlist	63
With DTR	None (quiet)	Manual connection	Hostlist	N/A
With DTR	None (quiet)	Autostart	Hostlist	65
With DTR	None (quiet)	UDP	Hostlist	N/A
With DTR	Character	No active startup	Hostlist	N/A
With DTR	Character	Any character	Hostlist	71
With DTR	Character	Active DTR	Hostlist	72
With DTR	Character	CR (0x0D)	Hostlist	73
With DTR	Character	Manual connection	Hostlist	N/A
With DTR	Character	Autostart	Hostlist	75
With DTR	Character	UDP	Hostlist	N/A
Unconditionally	None (quiet)	No active startup	Hostlist	N/A
Unconditionally	None (quiet)	Any character	Hostlist	E1
Unconditionally	None (quiet)	Active DTR	Hostlist	E2
Unconditionally	None (quiet)	CR (0x0D)	Hostlist	E3
Unconditionally	None (quiet)	Manual connection	Hostlist	N/A
Unconditionally	None (quiet)	Autostart	Hostlist	E5
Unconditionally	None (quiet)	UDP	Hostlist	N/A
Unconditionally	Character	No active startup	Hostlist	N/A
Unconditionally	Character	Any character	Hostlist	F1
Unconditionally	Character	Active DTR	Hostlist	F2
Unconditionally	Character	CR (0x0D)	Hostlist	F3
Unconditionally	Character	Manual connection	Hostlist	N/A
Unconditionally	Character	Autostart	Hostlist	F5
Unconditionally	Character	UDP	Hostlist	N/A

The following connect mode options are for when you use modem emulation:

Table 6-3. Connect Mode Options for Modem Emulation

Accept Incoming Connections	Response	Hex
Never	Echo	16
Never	Without echo	6
Never	1-character response	7
With DTR	Echo	56

With DTR	Without echo	46
With DTR	1-character response	47
Unconditionally	Echo	D6
Unconditionally	Without echo	C6
Unconditionally	1-character response	C7

Disconnect Mode Options

Table 6-4. Disconnect Mode Options

Disconnect with DTR Drop	Telnet Mode and Terminal Type Setup	Channel (port) Password	Hard Disconnect	State LED Off with Connection	Disconnect with EOT (^D)	Hex
			Enable			0
		Enable	Enable			10
			Enable		Enable	20
		Enable	Enable		Enable	30
	Enable		Enable			40
	Enable	Enable	Enable			50
	Enable		Enable		Enable	60
	Enable	Enable	Enable		Enable	70
Enable			Enable			80
Enable		Enable	Enable			90
Enable			Enable		Enable	A0
Enable		Enable	Enable		Enable	B0
Enable	Enable		Enable			C0
Enable	Enable	Enable	Enable			D0
Enable	Enable		Enable		Enable	E0
Enable	Enable	Enable	Enable		Enable	F0
			Enable	Enable		1
		Enable	Enable	Enable		11
			Enable	Enable	Enable	21
		Enable	Enable	Enable	Enable	31
	Enable		Enable	Enable		41
	Enable	Enable	Enable	Enable		51
	Enable		Enable	Enable	Enable	61
	Enable	Enable	Enable	Enable	Enable	71
Enable			Enable	Enable		81
Enable		Enable	Enable	Enable		91
Enable			Enable	Enable	Enable	A1
Enable		Enable	Enable	Enable	Enable	B1
Enable	Enable		Enable	Enable		C1
Enable	Enable	Enable	Enable	Enable		D1
Enable	Enable		Enable	Enable	Enable	E1
Enable	Enable	Enable	Enable	Enable	Enable	F1
			Disable			8
		Enable	Disable			18
			Disable		Enable	28
		Enable	Disable		Enable	38
	Enable		Disable			48
	Enable	Enable	Disable			58

Disconnect with DTR Drop	Telnet Mode and Terminal Type Setup	Channel (port) Password	Hard Disconnect	State LED Off with Connection	Disconnect with EOT (^D)	Hex
	Enable		Disable		Enable	68
	Enable	Enable	Disable		Enable	78
Enable			Disable			88
Enable		Enable	Disable			98
Enable			Disable		Enable	A8
Enable		Enable	Disable		Enable	B8
Enable	Enable		Disable			C8
Enable	Enable	Enable	Disable			D8
Enable	Enable		Disable		Enable	E8
Enable	Enable	Enable	Disable		Enable	F8
			Disable	Enable		9
		Enable	Disable	Enable		19
			Disable	Enable	Enable	29
		Enable	Disable	Enable	Enable	39
	Enable		Disable	Enable		49
	Enable	Enable	Disable	Enable		59
	Enable		Disable	Enable	Enable	69
	Enable	Enable	Disable	Enable	Enable	79
Enable			Disable	Enable		89
Enable		Enable	Disable	Enable	Enable	99
Enable			Disable	Enable	Enable	A9
Enable		Enable	Disable	Enable	Enable	B9
Enable	Enable		Disable	Enable		C9
Enable	Enable	Enable	Disable	Enable		D9
Enable	Enable		Disable	Enable	Enable	E9
Enable	Enable	Enable	Disable	Enable	Enable	F9

Flush Mode (Buffer Flushing) Options

Table 6-5. Flush Mode Options

Serial to Network Clear input buffer upon:	Network to Serial Clear output buffer upon:	Alternate Packing Algorithm	Hex
None			0
Active connection			10
Passive connection			20
Active connection Passive connection			30
Disconnect			40
Active connection Disconnect			50
Passive connection Disconnect			60
Active connection Passive connection Disconnect			70
		Enable	80
Active connection		Enable	90
Passive connection		Enable	A0
Active connection Passive connection		Enable	B0
Disconnect		Enable	C0
Active connection Disconnect		Enable	D0
Passive connection Disconnect		Enable	E0
Active connection Passive connection Disconnect		Enable	F0
	Active connection		1
Active connection	Active connection		11
Passive connection	Active connection		21
Active connection Passive connection	Active connection		31
Disconnect	Active connection		41
Active connection Disconnect	Active connection		51
Passive connection Disconnect	Active connection		61
Active connection Passive connection Disconnect	Active connection		71
	Active connection	Enable	81
Active connection	Active connection	Enable	91
Passive connection	Active connection	Enable	A1

Serial to Network Clear input buffer upon:	Network to Serial Clear output buffer upon:	Alternate Packing Algorithm	Hex
Active connection Passive connection	Active connection	Enable	B1
Disconnect	Active connection	Enable	C1
Active connection Disconnect	Active connection	Enable	D1
Passive connection Disconnect	Active connection	Enable	E1
Active connection Passive connection Disconnect	Active connection	Enable	F1
	Passive connection		2
Active connection	Passive connection		12
Passive connection	Passive connection		22
Active connection Passive connection	Passive connection		32
Disconnect	Passive connection		42
Active connection Disconnect	Passive connection		52
Passive connection Disconnect	Passive connection		62
Active connection Passive connection Disconnect	Passive connection		72
	Passive connection	Enable	82
Active connection	Passive connection	Enable	92
Passive connection	Passive connection	Enable	A2
Active connection Passive connection	Passive connection	Enable	B2
Disconnect	Passive connection	Enable	C2
Active connection Disconnect	Passive connection	Enable	D2
Passive connection Disconnect	Passive connection	Enable	E2
Active connection Passive connection Disconnect	Passive connection	Enable	F2
	Active connection Passive connection		3
Active connection	Active connection Passive connection		13
Passive connection	Active connection Passive connection		23
Active connection Passive connection	Active connection Passive connection		33
Disconnect	Active connection Passive connection		43
Active connection Disconnect	Active connection Passive connection		53

Serial to Network Clear input buffer upon:	Network to Serial Clear output buffer upon:	Alternate Packing Algorithm	Hex
Passive connection Disconnect	Active connection Passive connection		63
Active connection Passive connection Disconnect	Active connection Passive connection		73
	Active connection Passive connection	Enable	83
Active connection	Active connection Passive connection	Enable	93
Passive connection	Passive connection Active connection	Enable	A3
Active connection Passive connection	Active connection Passive connection	Enable	B3
Disconnect	Active connection Passive connection	Enable	C3
Active connection Disconnect	Active connection Passive connection	Enable	D3
Passive connection Disconnect	Active connection Passive connection	Enable	E3
Active connection Passive connection Disconnect	Active connection Passive connection	Enable	F3
	Disconnect		4
Active connection	Disconnect		14
Passive connection	Disconnect		24
Active connection Passive connection	Disconnect		34
Disconnect	Disconnect		44
Active connection Disconnect	Disconnect		54
Passive connection Disconnect	Disconnect		64
Active connection Passive connection Disconnect	Disconnect		74
	Disconnect	Enable	84
Active connection	Disconnect	Enable	94
Passive connection	Disconnect	Enable	A4
Active connection Passive connection	Disconnect	Enable	B4
Disconnect	Disconnect	Enable	C4
Active connection Disconnect	Disconnect	Enable	D4
Passive connection Disconnect	Disconnect	Enable	E4

Serial to Network Clear input buffer upon:	Network to Serial Clear output buffer upon:	Alternate Packing Algorithm	Hex
Active connection Passive connection Disconnect	Disconnect	Enable	F4
	Active connection Disconnect		5
Active connection	Active connection Disconnect		15
Passive connection	Active connection Disconnect		25
Active connection Passive connection	Active connection Disconnect		35
Disconnect	Active connection Disconnect		45
Active connection Disconnect	Active connection Disconnect		55
Passive connection Disconnect	Active connection Disconnect		65
Active connection Passive connection Disconnect	Active connection Disconnect		75
	Active connection Disconnect	Enable	85
Active connection	Active connection Disconnect	Enable	95
Passive connection	Active connection Disconnect	Enable	A5
Active connection Passive connection	Active connection Disconnect	Enable	B5
Disconnect	Active connection Disconnect	Enable	C5
Active connection Disconnect	Active connection Disconnect	Enable	D5
Passive connection Disconnect	Active connection Disconnect	Enable	E5
Active connection Passive connection Disconnect	Active connection Disconnect	Enable	F5
	Passive connection Disconnect		6
Active connection	Passive connection Disconnect		16
Passive connection	Passive connection Disconnect		26
Active connection Passive connection	Passive connection Disconnect		36
Disconnect	Passive connection Disconnect		46
Active connection Disconnect	Passive connection Disconnect		56

Serial to Network Clear input buffer upon:	Network to Serial Clear output buffer upon:	Alternate Packing Algorithm	Hex
Passive connection Disconnect	Passive connection Disconnect		66
Active connection Passive connection Disconnect	Passive connection Disconnect		76
	Passive connection Disconnect	Enable	86
Active connection	Passive connection Disconnect	Enable	96
Passive connection	Passive connection Disconnect	Enable	A6
Active connection Passive connection	Passive connection Disconnect	Enable	B6
Disconnect	Passive connection Disconnect	Enable	C6
Active connection Disconnect	Passive connection Disconnect	Enable	D6
Passive connection Disconnect	Passive connection Disconnect	Enable	E6
Active connection Passive connection Disconnect	Passive connection Disconnect	Enable	F6
	Active connection Passive connection Disconnect		7
Active connection	Active connection Passive connection Disconnect		17
Passive connection	Active connection Passive connection Disconnect		27
Active connection Passive connection	Active connection Passive connection Disconnect		37
Disconnect	Active connection Passive connection Disconnect		47
Active connection Disconnect	Active connection Passive connection Disconnect		57
Passive connection Disconnect	Active connection Passive connection Disconnect		67
Active connection Passive connection Disconnect	Active connection Passive connection Disconnect		77
	Active connection Passive connection Disconnect	Enable	87

Serial to Network Clear input buffer upon:	Network to Serial Clear output buffer upon:	Alternate Packing Algorithm	Hex
Active connection	Active connection Passive connection Disconnect	Enable	97
Passive connection	Active connection Passive connection Disconnect	Enable	A7
Active connection Passive connection	Active connection Passive connection Disconnect	Enable	B7
Disconnect	Active connection Passive connection Disconnect	Enable	C7
Active connection Disconnect	Active connection Passive connection Disconnect	Enable	D7
Passive connection Disconnect	Active connection Passive connection Disconnect	Enable	E7
Active connection Passive connection Disconnect	Active connection Passive connection Disconnect	Enable	F7

Interface Mode Options

Table 6-6. Interface Mode Options

Interface	Bits	Parity	Stop Bits	Hex
RS-232C	7	No	1	48
RS-232C	7	No	2	C8
RS-232C	7	Even	1	78
RS-232C	7	Even	2	F8
RS-232C	7	Odd	1	58
RS-232C	7	Odd	2	D8
RS-232C	8	No	1	4C
RS-232C	8	No	2	CC
RS-232C	8	Even	1	7C
RS-232C	8	Even	2	FC
RS-232C	8	Odd	1	5C
RS-232C	8	Odd	2	DC
RS-422/485	7	No	1	49
RS-422/485	7	No	2	C9
RS-422/485	7	Even	1	79
RS-422/485	7	Even	2	F9
RS-422/485	7	Odd	1	59
RS-422/485	7	Odd	2	D9
RS-422/485	8	No	1	4D
RS-422/485	8	No	2	CD
RS-422/485	8	Even	1	7D
RS-422/485	8	Even	2	FD
RS-422/485	8	Odd	1	5D
RS-422/485	8	Odd	2	DD
RS-422/485 2-Wire	7	No	1	4B
RS-422/485 2-Wire	7	No	2	CB
RS-422/485 2-Wire	7	Even	1	7B
RS-422/485 2-Wire	7	Even	2	FB
RS-422/485 2-Wire	7	Odd	1	5B
RS-422/485 2-Wire	7	Odd	2	DB
RS-422/485 2-Wire	8	No	1	4F
RS-422/485 2-Wire	8	No	2	CF
RS-422/485 2-Wire	8	Even	1	7F
RS-422/485 2-Wire	8	Even	2	FF
RS-422/485 2-Wire	8	Odd	1	5F
RS-422/485 2-Wire	8	Odd	2	DF

Pack Control Options

Table 6-7. Pack Control Options

Sendcharacter Defined by a:	Trailing Characters	Idle Time Force Transmit:	Send Immediately after Sendcharacter	Hex
1-Byte Sequence	No	12ms		0
1-Byte Sequence	No	52ms		1
1-Byte Sequence	No	250ms		2
1-Byte Sequence	No	5sec		3
1-Byte Sequence	1	12ms		4
1-Byte Sequence	1	52ms		5
1-Byte Sequence	1	250ms		6
1-Byte Sequence	1	5sec		7
1-Byte Sequence	2	12ms		8
1-Byte Sequence	2	52ms		9
1-Byte Sequence	2	250ms		A
1-Byte Sequence	2	5sec		B
2-Byte Sequence	No	12ms		10
2-Byte Sequence	No	52ms		11
2-Byte Sequence	No	250ms		12
2-Byte Sequence	No	5sec		13
2-Byte Sequence	1	12ms		14
2-Byte Sequence	1	52ms		15
2-Byte Sequence	1	250ms		16
2-Byte Sequence	1	5sec		17
2-Byte Sequence	2	12ms		18
2-Byte Sequence	2	52ms		19
2-Byte Sequence	2	250ms		1A
2-Byte Sequence	2	5sec		1B
1-Byte Sequence	No	12ms	Yes	20
1-Byte Sequence	No	52ms	Yes	21
1-Byte Sequence	No	250ms	Yes	22
1-Byte Sequence	No	5sec	Yes	23
1-Byte Sequence	1	12ms	Yes	24
1-Byte Sequence	1	52ms	Yes	25
1-Byte Sequence	1	250ms	Yes	26
1-Byte Sequence	1	5sec	Yes	27
1-Byte Sequence	2	12ms	Yes	28
1-Byte Sequence	2	52ms	Yes	29
1-Byte Sequence	2	250ms	Yes	2A
1-Byte Sequence	2	5sec	Yes	2B
2-Byte Sequence	No	12ms	Yes	30
2-Byte Sequence	No	52ms	Yes	31

Sendcharacter Defined by a:	Trailing Characters	Idle Time Force Transmit:	Send Immediately after Sendcharacter	He x
2-Byte Sequence	No	250ms	Yes	32
2-Byte Sequence	No	5sec	Yes	33
2-Byte Sequence	1	12ms	Yes	34
2-Byte Sequence	1	52ms	Yes	35
2-Byte Sequence	1	250ms	Yes	36
2-Byte Sequence	1	5sec	Yes	37
2-Byte Sequence	2	12ms	Yes	38
2-Byte Sequence	2	52ms	Yes	39
2-Byte Sequence	2	250ms	Yes	3A
2-Byte Sequence	2	5sec	Yes	3B