LANTRONIX®

XPort™

XPort™ User Guide

Part Number 900-270
Revision C 11/03

Copyright and Trademark

XPort, with its patent-pending technology, is a trademark of Lantronix.

Ethernet is a trademark of XEROX Corporation. UNIX is a registered trademark of The Open Group. Windows 95, Windows 98, Windows 2000, Windows NT, and Windows XP are trademarks of Microsoft Corp. Netscape is a trademark of Netscape Communications Corporation.

Contacts

Lantronix Corporate Headquarters
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 and 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.

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

Attention: *With the purchase of XPort™, the OEM agrees to an OEM firmware license agreement that grants the OEM a non-exclusive, royalty-free firmware license to use and distribute the binary firmware image provided, only to the extent necessary to use the XPort™ hardware. For further details, please see the XPort OEM firmware license agreement.*

Date	Rev.	Comments
11/03	C	Revised for v.1.5 of the firmware. We consolidated software documentation in this user guide; hardware information is now in the XPort Integration Guide.

If you use a previous version of the firmware, go to the Lantronix FTP site at ftp://ftp.lantronix.com/pub to find the earlier documentation.

Contents

1: Using This Guide

Purpose and Audience

This guide provides the information needed to configure, use and update the XPort™ and is intended for software developers and system integrators who are embedding the XPort™ in their designs. The information in this guide is relevant to XPort with firmware version 1.5 and higher.

Chapter Summary

The remaining chapters in this guide include:

2:Introduction	Describes the main features of the XPort and the protocols it supports.
3:Getting Started	Provides information for getting your unit up and running, using DeviceInstaller to assign an IP address, and Web-Manager to set parameters such as port and server properties.
4:Using Setup Mode	Provides instructions for accessing Setup Mode (command line interface) using a Telnet connection through the network or a terminal or terminal emulation program through the serial port. Details the parameters that you must configure.
5:GPIO Interface	Provides instructions for configuring the three General Purpose I/O pins (CP1-3).
6:Updating Firmware	Provides instructions for obtaining the latest firmware and updating the XPort.
7:Monitoring the Network	Provides instructions for accessing and using the command line interface for monitoring the network and diagnosing problems.
8:Troubleshooting	Describes common problems and error messages and how to contact Lantronix Technical Support.
9:IP Addresses	Provides detailed information about IP addressing and the components of an IP address.
A: Binary to Hex Conversion	Provides tables for converting from binary numbers to the hexadecimal notation needed when setting some parameters.
B: Networking Terms	Defines common networking terms.

Additional Documentation

The following guides are available on the product CD and the Lantronix web site (www.lantronix.com)

XPort Quick Start	Provides the steps for getting the XPort evaluation board up and running.
XPort Integration Guide	Provides information about the XPort hardware, testing the XPort using the evaluation board, and integrating the XPort into your product.
DeviceInstaller User Guide	Provides instructions for using the Windows-based utility to configure the XPort and other Lantronix device servers.
Com Port Redirector User Guide	Provides information on using the Windows-based utility to create a virtual com port.
Creating Custom Web Pages	Explains the detailed requirements for adding web services to your XPort and to other Lantronix device servers.

2: Introduction

This chapter familiarizes you with what the XPort device server can do and some basic information you need to know before you get started.

Capabilities

The XPort device server has the following capabilities:

- Connects devices through a TCP data channel or through a Telnet connection to computers or to another device server. The XPort can also send UDP datagrams.
- Contains a web [HTTP] server that allows presentation of custom content and easy configuration through the browser.
- Has three programmable IO pins that can be used to monitor or control attached devices.

Applications

The XPort device server connects serial devices such as those listed below to Ethernet networks using the IP protocol family.

- ATM machines
- CNC controllers
- Data collection devices
- Universal Power Supply (UPS) management units
- Telecommunications equipment
- Data display devices
- Security alarms and access control devices
- Handheld instruments
- Modems
- Time/attendance clocks and terminals

Protocol Support

The XPort device server uses the Internet Protocol (IP) for network communications. It uses 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 include:

- ARP, UDP, TCP, ICMP, Telnet, TFTP, AutoIP, DHCP, HTTP, and SNMP for network communications and management.
- TCP, UDP, and Telnet for connections to the serial port.
- TFTP for firmware and web page 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.
- SMTP for e-mail transmission.

Addresses and Port Numbers

Hardware Address

The hardware address is also referred to as the Ethernet 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.

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

IP Address

Every device connected to an IP network must have a unique IP address. This address is used to reference the specific unit. (See 9:IP Addresses for further explanation of IP addresses.)

Port Numbers

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 phone 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.

Logon Methods

For the unit to operate correctly on a network, it must have a unique IP address on the network. There are three basic methods for logging into the device server and assigning the IP address:

DeviceInstaller: You manually assign the IP address using a graphical user interface (GUI) on a PC attached to a network. (See 3:Getting Started.)

Network Port Login: Make a Telnet connection to the network port (9999). (See 4:Using Setup Mode.*)*

Serial Port Login: Connect a terminal or a PC running a terminal emulation program to the unit's serial port (CH 1). (See 4:Using Setup Mode.*)*

3: Getting Started

This chapter covers the steps for getting the XPort device server online and working. It includes the following topics:

Required Information

Hardware Address

You need to know the unit's hardware address (also known as MAC address), which is on the product label. It is in the format: 00-20-4a-XX-XX-XX, where the XXs are unique numbers assigned to the product.

Hardware Address: 00-20-4a-_____-_____-_____

IP Address

Your XPort must have a unique IP address on your network. The systems administrator generally provides the IP address and corresponding subnet mask and gateway. The IP address must be within a valid range, unique to your network, and in the same subnet as your PC.

IP Address: _____ _____ _____ _____

Subnet Mask: _____ _____ _____ _____

Gateway: _____ _____ _____ _____

Using DeviceInstaller to Assign an IP Address

The unit's IP address must be configured before it can work correctly on a network. You have several options for assigning an IP to your unit. We recommend that you manually assign the IP address over the network using DeviceInstaller software, which is on the product CD.

Note: *For information about the other methods, see 9:IP Addresses. If you want to use a serial connection instead of an Ethernet connection to configure the device, see Using the Serial Port on page 4-2.*

Installing DeviceInstaller

1. Open DeviceInstaller on the CD-ROM.

   If the CD does not launch automatically:

   a. Click the **Start** button on the Task Bar and select **Run**.

   b. Enter your CD drive letter, colon, backslash, **Launch.exe** (e.g., D:\Launch.exe).

2. Respond to the installation wizard prompts.

Note: *For more information about DeviceInstaller, see the DeviceInstaller User Guide on the product CD and the DeviceInstaller help file.*

Assigning an IP Address

The unit's IP address is normally set to 0.0.0.0 at the factory. The hardware address is on the product label. The unit is DHCP enabled as the default.

To manually assign an IP address:

1. Click **Start→Programs → Lantronix→DeviceInstaller→DeviceInstaller.** If your PC has more than one network adapter, a message displays. Select an adapter and click **OK**.

   Note: *If the unit already has an IP address (e.g., DHCP has assigned an IP address), click the* ***Search*** *icon and select the unit from the list of Lantronix device servers on the local network.*

2. Click the **Assign IP** icon 

.
3. If prompted, enter the hardware address (on the product label) and click **Next**.
4. Select **Assign a specific IP address** and click **Next**.
5. Enter the **IP address**. The **Subnet mask** displays automatically based on the IP address; if desired, you may change it. On a local network, you can leave the **Default gateway** blank (all zeros). Click **Next**.
6. Click the **Assign** pushbutton and wait several seconds until a confirmation message displays. Click **Finish**.

7. Select the XPort from the main window list and click **Tools→Ping**. The results display in the Status area. Click the **Clear Status** button to clear the window so you can ping the device again.

   Note: *If you do not receive "Reply" messages, make sure the unit is properly attached to the network and that the IP address assigned is valid for the particular network segment you are working with.*

8. Click the **Close** pushbutton.

Using Web-Manager to Configure 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.

The unit's configuration is stored in nonvolatile memory and is retained without power. You can change the configuration at any time. The unit performs a reset after you change and store the configuration.

In this chapter, we describe how you can configure the XPort using Web-Manager, Lantronix's browser-based configuration tool. (For information on using Setup Mode, our command line configuration interface, see 4:Using Setup Mode on page 4-1.)

Note: *The examples in this section show a typical device. Your device may have different configuration options.*

To configure the unit:

1. Open DeviceInstaller.
2. Click the **Search** icon 

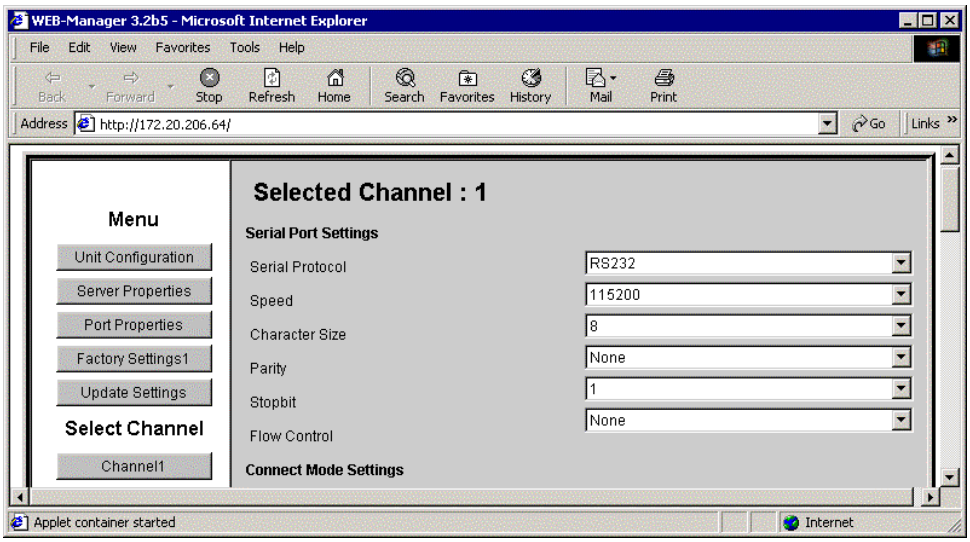
. A list of Lantronix device servers on the network displays.
3. Select the unit and click the **Web** icon 

, or select **Web Pages** from the **Device** menu.

   The Lantronix Web-Manager window displays in your browser.

   Note: *You can also open your JAVA enabled web browser and enter the IP address of the XPort to open Web-Manager.*

Figure 1-1. Lantronix Web-Manager



On the left, Web-Manager has the following menu options (pushbuttons):

- Unit Configuration
- Server Properties
- Port Properties
- Factory Settings1
- Update Settings
- Select Channel

4. Use the Menu to navigate to sub pages where you can configure server settings.
5. When you are finished, click the **Update Settings** button to save your settings.

Notes:

- *The next chapter, 4:Using Setup Mode, explains the configuration settings in detail.*
- *You must use Setup Mode to configure e-mail, expert, and security settings. You must use DeviceInstaller for the configurable pins' settings.*

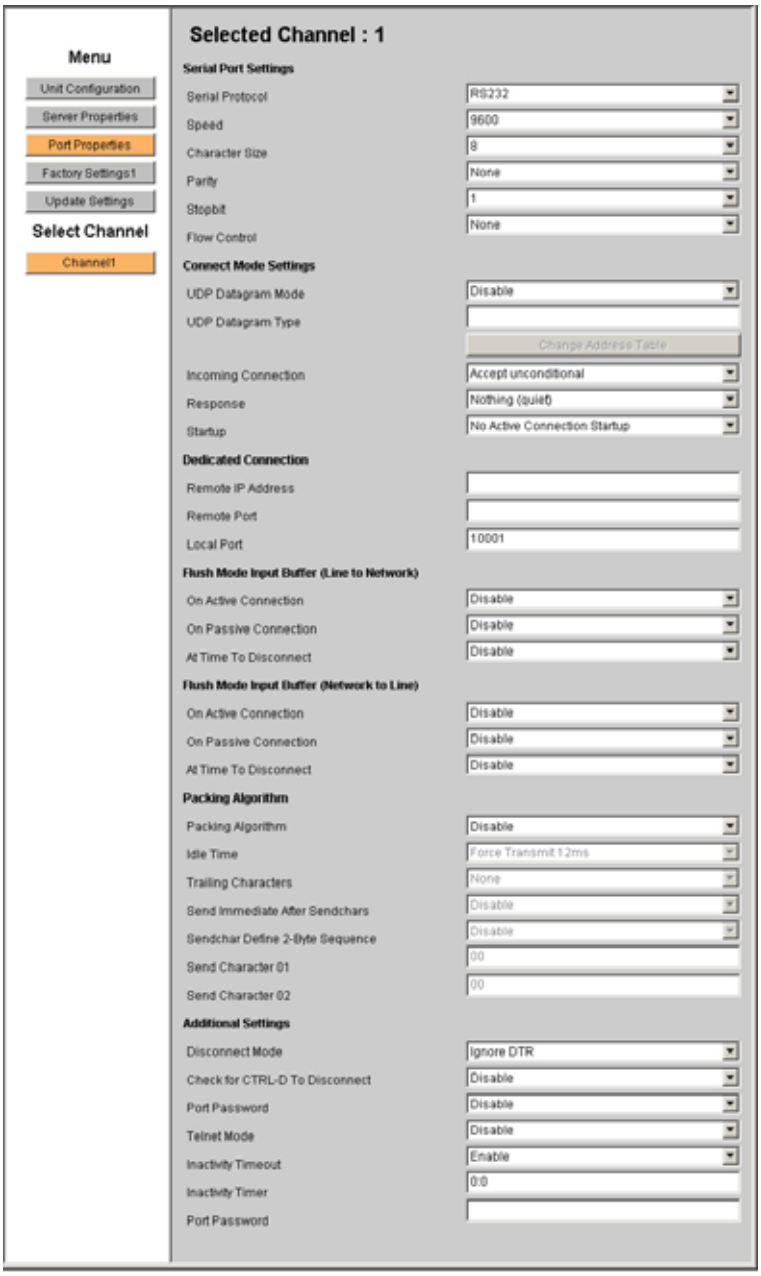
Unit Configuration Settings

Click the **Unit Configuration** button to display the following page. This page contains the Server Configuration and the Port Configuration settings. These are the current settings read from the device.

Note: *The following examples represent typical web pages. See the Lantronix web site for the latest version.*

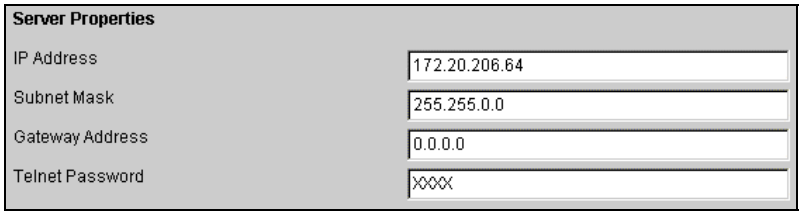
The following figure shows the information available on the Unit Configuration web page.

Figure 1-3. Unit Configuration Web Page



Server Properties

You can change the server properties by editing any of the fields. Holding the cursor over a field displays a help message for that field. If you change the IP address, you must enter the new IP address in the browser to reload the page.

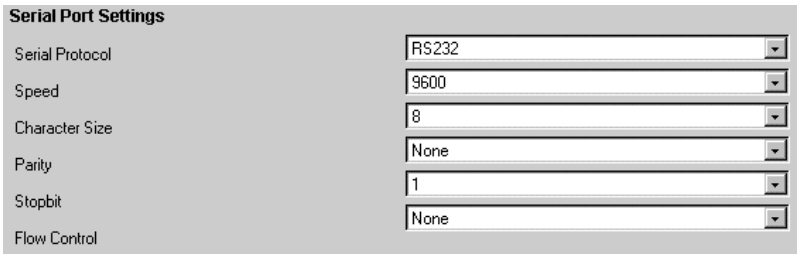


In the **Telnet Password** field, enter a password to prevent unauthorized access to the Setup Mode via a Telnet connection to port 9999. The password is limited to 4 characters. (An enhanced password setting of 16 characters is available under Security Settings on the Telnet Setup Mode window.)

Note: *You do not need a password to access the Setup Mode window via a serial connection.*

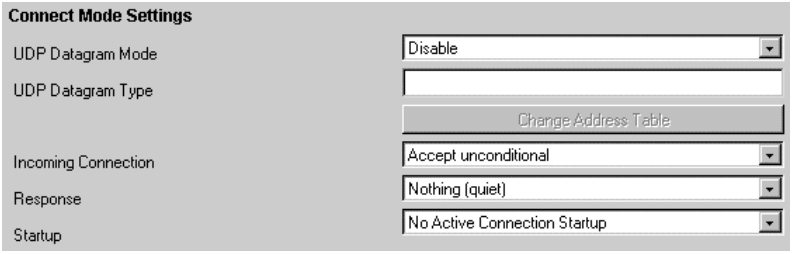
Port Properties

Serial Port Settings



Serial Protocol	RS232 ***Note:*** *RS-232 is the only available option for XPort.*
Speed	300, 600, 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200, 230400
Character Size	8, 7
Parity	None, Even, Odd
Stop Bit	1,2
Flow Control	None, XON/XOFF, XON/XOFF Pass Characters to Host, CTS/RTS (Hardware)

Connect Mode Settings



UDP Datagram Mode Enable, Disable

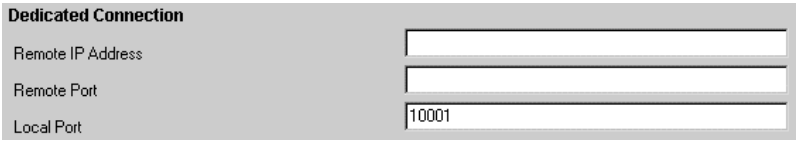
UDP Datagram Type User Selectable

Incoming Connection Accept unconditional, Accept incoming/DTR, Never accept incoming

Response Nothing (quiet), Character Response

Startup No Active Connection Startup, With Any Character, With a Specific Start Character, Manual Connection, Autostart, Modem Mode, With Active DTR

Dedicated Connection

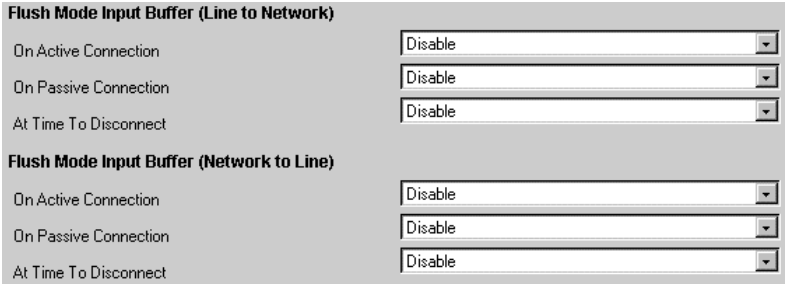


Remote IP Address User selectable

Remote Port User selectable

Local Port User selectable (default 10001)

Flush Mode Input Buffer

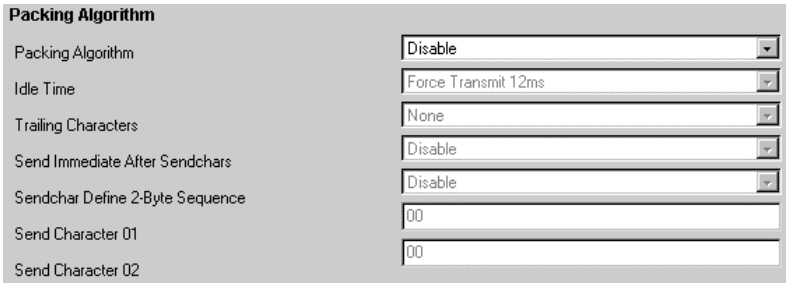


On Active Connection Enable, Disable

On Passive Connection Enable, Disable

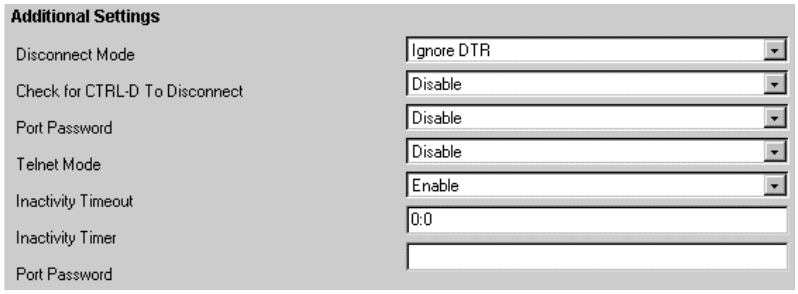
At Time To Disconnect Enable, Disable

Packing Algorithm



Packing Algorithm	Enable, Disable
Packing Interval	Interval 12 ms, Interval 52 ms, Interval 250 ms, Interval 5000 ms
Trailing Characters	None, One, Two
Send Immediate After Sendchars	Enable, Disable
Sendchar Define2-Byte Sequence	Enable, Disable
Send Character 01	User selectable
Send Character 02	User selectable

Additional Settings



Disconnect Mode	Ignore DTR, With DTR Drop
Check for CTRL-D to Disconnect	Enable, Disable
Port Password	Enable, Disable
Telnet Mode	Enable, Disable
Inactivity Timeout	Enable, Disable
Inactivity Timer	User Selectable
Port Password	User selectable; Port Password must be enabled

Factory Settings

Click the **Factory Settings** button to set the device server back to the factory default settings.

Note: *Factory Settings resets factory settings for the channel. This option does not change the IP address, gateway, and subnet mask to the factory default values.*

Update Settings

Click the **Update Settings** button to send all changed settings to the device.

4: Using Setup Mode for Configuration

You must configure the unit so that it can communicate on a network with your serial device. You can configure it using a web browser, as described in 3:Getting Started, or locally or remotely using the following procedures:

- 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 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.

Note: *The menus in this section show a typical device. Your device may have different configuration options.*

This chapter includes the following topics:

Accessing Setup Mode

Using a Telnet Connection

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

Note: *You can also use DeviceInstaller to access Telnet. Select the device from the main window list, and click the* ***Telnet*** *icon* 

. If you use the ***Telnet*** *icon on the DeviceInstaller toolbar, skip steps 1 and 2.*

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:

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

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

2. Click **OK**. The following information displays.

Figure 4-1. MAC Address

```
MAC address 00204A41164D
Software version 01.3b1 (030605) XPTE

Press Enter to go into Setup Mode
```

3. To enter the Setup Mode, **press Enter within 5 seconds**. The configuration settings display, followed by the setup menu options.

Figure 4-2. Setup Menu Options

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

4. Select an option on the menu by entering the number of the option in the **Your choice** ? field and pressing **Enter**.
5. To enter a value for a parameter, type the value and press **Enter**, or to confirm a current value, just press **Enter**.
6. When you are finished, save the new configurations (option 9). The unit reboots.

Using the Serial Port

To initially configure the unit through a serial connection:

1. Connect a console terminal or PC running a terminal emulation program to your unit's 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, reset the unit, either by pushing the red reset button, or cycling the unit's power (power off and back on). The self-test will begin. **You have one second** to enter three lowercase **x** characters (**xxx**).

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

3. At this point, the screen display is the same as when you use a Telnet connection. To continue, go to step 4 in Using a Telnet Connection on page 4-1.

The figure below shows all of the configuration parameters. The remainder of this chapter describes each parameter in detail.

Figure 4-4. Setup Mode Configuration Parameters

```
*** basic parameters
Hardware: Ethernet TPI
IP addr 172.19.23.60, gateway 172.019.000.001,netmask 255.255.000.000

*** 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          disabled
Enhanced Password is disabled
Port 77F0h is          enabled

*** Channel 1
Baudrate 115200, I/F Mode 4C, Flow 00
Port 14009
Remote IP Adr: --- none ---, Port 00000
Connect Mode : C0
Disconn Mode : 00
Flush   Mode : 00

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

**************** E-mail ******************
Mail server: 0.0.0.0
Unit       :
Domain     :
Recipient 1:
Recipient 2:

*** Trigger 1
Serial Sequence: 00,00
CP1: X
CP2: X
CP3: X
Message :
Priority: L
Min. notification interval: 1 s
Re-notification interval  : 0 s

*** Trigger 2
Serial Sequence: 00,00
CP1: X
CP2: X
CP3: X
Message :
Priority: L
Min. notification interval: 1 s
Re-notification interval  : 0 s

*** Trigger 3
Serial Sequence: 00,00
CP1: X
CP2: X
CP3: X
Message :
Priority: L
Min. notification interval: 1 s
Re-notification interval  : 0 s
```

Server Configuration (Network Configuration)

The unit's basic network parameters display when you select **Server configuration** (option **0**). The **IP Address**, **Set Gateway IP Address**, and **Netmask** fields display the current values.

Figure 4-6. Server Configuration Parameters

```
IP Address : (000) .(000) .(000) .(000)
Set Gateway IP Address (N)
Netmask: Number of Bits for Host Part (0=default)  (0)
Change telnet config password (N)
```

IP Address

The IP address must be set to a unique value in your network. (See 9:IP Addresses for more information.)

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. The default is N (No), meaning the gateway address has not been set. To set the gateway address, type **Y** and enter the address.

Netmask: Number of Bits for Host Part

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 displays in standard decimal-dot notation when the saved parameters are displayed (for example, 255.255.255.0).

Table 4-1. 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

Change Telnet Configuration Password

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

Note: *You don't need a password to access the Setup Mode window via a serial connection.*

DHCP Name

If a DHCP server has automatically assigned the IP address and network settings, you can discover the unit by using the DeviceInstaller network search feature.

There are three methods for assigning DHCP names to the unit.

- **Default DHCP Name**: If you do not change the DHCP name, and you are using an IP of 0.0.0.0, then the DHCP name defaults to CXXXXXX (XXXXXX is the last 6 digits of the MAC address shown on the label on the bottom/side of the unit). For example, if the MAC address is 00-20-4A-12-34-56, then the default DHCP name is C123456.
- **Custom DHCP Name**: You can create your own DHCP name. If you are using an IP address of 0.0.0.0, then the last option in Server configuration is **Change DHCP device name**. This option allows you to change the DHCP name to an alphanumeric name (LTX in our example).

Figure 4-8. Custom DHCP Name

```
Change DHCP device name (not set) ? (N) Y
Enter new DHCP device name : LTX
```

- **Numeric DHCP Name:** You can change the DHCP name by specifying the last octet of the IP address. When you use this method, the DHCP name is LTXYY where YY is what you chose for the last octet of the IP address. If the IP address you specify is 0.0.0.12, then the DHCP name is LTX12. This method only works with 2 digit numbers (0-99).

Channel 1 Configuration (Serial Port Parameters)

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

Note: *You must enter some values in hexadecimal notation. For information on converting from binary to hexadecimal, see A::Binary to Hex Conversion.*

Figure 4-10. Serial Port Parameters

```
Baudrate (115200) ?
I/F Mode (4C) ?
Flow (00) ?
Port No (14009) ?
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, 115200, and 230400 bits per second.

I/F (Interface) Mode

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

Table 4-5. Interface Mode Options

I/F Mode Option	7	6	5	4	3	2	1	0
RS-232C (1)							0	0
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 bits(1)	1	1						

(1) 2 stop bits are implemented by the software. This might influence performance.

Note: *If you attempt to select an I/F Mode bit that pertains to RS-422/485, a WARNING: RS-422/485 I/F Modes not supported message displays.*

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

Table 4-8. 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

Flow

Flow control sets the local handshaking method for stopping serial input/output. Generally, flow control is not required if the connection is used to pass a blocked protocol with block sizes less than 1k (ACK/NAK) and/or speeds of 19200 or less. Use the following table to select flow control options:

Table 4-11. 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 4-14. Reserved Port Numbers

Port Numbers	Reserved for
1 – 1024	Reserved (well known ports)
9999	Telnet setup
14000-14009	Reserved for Redirector
30704	Reserved (77F0h)
30718	Reserved (77FEh)

Note: ***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, the initial value of 5000 actively establishes a connection. Each subsequent connection increments the number by 1. When the port number reaches 7999, it wraps around to 5000.

Only use the automatic port increment feature to initiate a connection using TCP. Set the port 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.

Table 4-15. Connect Mode Options

Connect Mode Option	7	6	5	4	3	2	1	0
Incoming Connection								
Never accept incoming	0	0	0					
Accept with DTR Active	0	1	0					
Always Accept	1	1	0					
Response								
Nothing (quiet)				0				
Character response (C=connect, D=disconnect, N=unreachable)				1				
Active Startup								
No active startup					0	0	0	0
With any character					0	0	0	1
With DTR Active					0	0	1	0

Connect Mode Option	7	6	5	4	3	2	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

Incoming Connection

Never Accept Incoming — Rejects all external connection attempts.

Accept with DTR Active — Accepts external connection requests only when the DTR input is asserted. Cannot be used with Modem Mode.

Always Accept — Accepts any incoming connection when a connection is not already established. Default setting.

Response

Character Response — A single character is transmitted to the serial port when there is a change in connection state:
C = connected, D = disconnected, N = host unreachable.
This option is overridden when the Active Start Modem Mode or Active Start Host List is in effect. Default setting is Nothing (quiet).

No Active Startup — Does *not* attempt to initiate a connection under any circumstance. Default setting.

With Any Character — Attempts to connect when any character is received from the serial port.

With DTR Active — Attempts to connect when the DTR input changes from not asserted to asserted.

With a Specific Start Character — Attempts to connect when it receives a specific start character from the serial port. The default start character is carriage return.

Manual Connection

Attempts to connect when directed by a command string received from the serial port. The first character of the command string must be a **C** (ASCII 0x43), and the last character must be either a carriage return (ASCII 0x0D) or a line feed (0x0A). No blanks or space characters may be in the command string. Between the first and last command string characters must be a full or partial destination IP address and may be a destination port number.

The IP address must be in standard dot-decimal notation and may be a partial address, representing the least significant 1, 2, or 3 bytes of the remote IP address. The period is required between each pair of IP address numbers.

If present, the port number must follow the IP address, must be presented as a decimal number in the range 1-65535, and must be preceded by a forward slash (ASCII 0x2F). The slash separates the IP address and the port number. If you omit the port number from a command string, the internally stored remote port number starts a connection.

If a partial IP address is presented in a command string, it is interpreted to be the least significant bytes of the IP address and uses the internally stored remote IP address to provide the most significant bytes of the IP address. If the IP address entered is 0.0.0.0/0, the device server enters Monitor Mode.

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 4-18. 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
C0.0.0.0/0	Connect to 129.1.28.10, port 12; enter Monitor Mode

Autostart (Automatic Connection)

If you enable autostart, the unit automatically connects to the remote IP address and remote port specified when the firmware starts.

Hostlist

If you enable this option, the device server 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.

Hostlist supports a minimum of 1 and a maximum of 12 entries. Each entry contains the IP address and the port number. The hostlist is disabled for Manual Mode and for Modem Mode. The unit will not accept a data connection from a remote device when the hostlist option is enabled.

Figure 4-12. Hostlist Option

```
Change Setup:
  0 Server configuration
  1 Channel 1 configuration
  3 E-mail settings
  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) 0.(000) 1     Port :
(0) ?23
02. IP address : (000) 172.(000) 19.(000) 0.(000) 2     Port :
(0) ?3001
03. IP address : (000) 172.(000) 19.(000) 0.(000) 3     Port :
(0) ?10001
04. IP address : (000) .(000) .(000) .(000)

Hostlist :
01. IP : 172.019.000.001  Port : 00023
02. IP : 172.019.000.002  Port : 03001
03. IP : 172.019.000.003  Port : 10001

Change Hostlist ? (N) N

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

To enable the hostlist:

1. Enter a **Connect Mode** of 0x20 (**2**X), where X is any digit. 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. The range is 1-15, with the default set to 3.

5. For **Retrytimeout**, enter the number of seconds the unit should wait before failing an attempted connection. The time is stored as units of milliseconds in the range of 1-65535. The default is 250.

Datagram Type

Directed UDP

When selecting this option, you are prompted for the Datagram type. Enter **01** for directed or broadcast UDP.

When the UDP option is in effect, the unit never attempts to initiate a TCP connection because it uses UDP datagrams to send and receive data.

Modem Mode

In Modem (Emulation) 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 XPorts, and to use an Ethernet connection instead of a phone call. By not having to change communications applications, you avoid 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).*

Without Echo	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 (without echo) refers to the modem *not* sending an answer to the commands received (or displaying what was typed).
Full Verbose	The unit echoes modem commands and responds to a command with a message string shown in the table below.
1-Character Response	The unit echoes modem commands and responds to a command with a single character response.

Table 4-21. Modem Mode Messages

Message	Meaning
Full Verbose	
OK	Command was executed without error.
CONNECT	A network connection has been established.
NO CARRIER	A network connection has been closed.
RING n.n.n.n.	A remote device, having IP address n.n.n.n, is connecting to this device.
1-Character Response	
0	OK
1	Connected
2	Ring
3	No Carrier
4	Error

Received commands must begin with the two-character sequence **AT** and be terminated with a carriage return character.

The unit ignores any character sequence received *not* starting with AT, and only recognizes and processes single AT-style commands. The unit treats compound AT commands as unrecognized commands.

If the Full Verbose option is in effect, the unit responds to an unrecognized command string that is otherwise formatted correctly (begins with AT and ends with carriage return) with the *OK* message and takes no further action.

If the 1-Character Response option is in effect, the unit responds to an unrecognized command string that is otherwise formatted correctly with *OK* and takes no further action.

When an active connection is in effect, the unit transfers data and does not process commands received from the serial interface.

When a connection is terminated or lost, the unit reverts to command mode.

When an active connection is in effect, the unit terminates the connection if it receives the following sequence from the attached serial device:

- No serial data is received for one second.
- The character sequence +++ is received, with no more than one second between each two characters.
- No serial data is received for one second after the last + character. At this time, the unit responds affirmatively per the selected echo/response mode.
- The character string **ATH** is received, terminated with a carriage return. The unit responds affirmatively according to the selected echo/response mode and drops the network connection. The serial interface reverts to accepting command strings.

If this sequence is not followed, the unit remains in data transfer mode.

Table 4-24. 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).
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: *The unit recognizes these AT commands as single commands such as ATE0 or ATV1; it does not recognize compound commands such as ATE0V.*

Remote IP Address

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

Remote Port

You must set the remote TCP port number 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

This setting determines the conditions under which the unit will cause a network connection to terminate.

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

Table 4-27. Disconnect Mode Options

Disconnect Mode Option	7	6	5	4	3	2	1	0
Disconnect with DTR drop (6)	1							
Ignore DTR	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 XPort sends 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 closes 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 turns off instead of blinking.
(5) When **Ctrl D** or Hex 04 is detected, the connection is dropped. Both Telnet mode and Disconnect with EOT must be enabled for Disconnect with EOT to function properly. **Ctrl D** is only detected going from the serial port to the network.
(6) When DTR transitions from a high state to a low state, the network connection to or from the serial port drops.

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.

Table 4-30. Flush Mode Options

Function	7	6	5	4	3	2	1	0
Input Buffer (Serial to Network)								
Clear with a connection that is initiated from the device to the network				1				
Clear with a connection initiated from the network to the device			1					
Clear when the network connection to or from the device is disconnected		1						
Output Buffer (Network to Serial)								
Clear with a connection that is initiated from the device to the network								1
Clear with a connection initiated from the network to the device							1	
Clear when the network connection to or from the device is disconnected						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 you do not need specific functions.

Table 4-33. Pack Control Options

Option	7	6	5	4	3	2	1	0
Packing Interval								
Interval: 12ms							0	0
Interval: 52ms							0	1
Interval: 250ms							1	0
Interval: 5sec							1	1
Trailing Characters								
None					0	0		
One					0	1		
Two					1	0		

Option	7	6	5	4	3	2	1	0
Send Characters								
2-Byte Send Character Sequence				1				
Send Immediately After Send chars			1					

Packing Interval: Packing Interval defines how long the unit should wait before sending accumulated characters. This wait period is between successive network segments containing data. For alternate packing, the default interval is 12 ms.

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 this option is not enabled, the unit interprets them independently.
- If Send Immediately After Characters is *not* set, any characters already in the serial buffer are included in the transmission after a "transmit" condition is found. If this option is 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 unit drops the connection if there is no activity on the serial line before the set time expires. Enter time in the 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**. Range is 0 (disabled) to 5999 seconds (99 minutes, 59 seconds). Default is 0.

Send Characters

You can enter up to two characters in hexadecimal representation in "sendchar." If the unit receives a character on the serial line that matches one of these characters, it sends the character immediately, along with any awaiting characters, to the TCP connection. This action minimizes the response time for specific protocol characters on the serial line (for example, ETX, EOT). Setting the first sendchar to **00** disables the recognition of the characters. Alternatively, the unit can interpret two characters as a sequence (see Pack Control on page 4-15).

Telnet Terminal Type

This parameter displays only if you enabled the terminal type option in Disconnect Mode. 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. If the option is enabled, you can set a password on the serial port.

E-mail Settings

Note: *You can change these settings via Telnet or serial connections only, not on the Web-Manager. To configure e-mail settings via DeviceInstaller, see E-mail Notification in the DeviceInstaller User Guide on the CD.*

The unit can send an e-mail to multiple recipients when a specific trigger event occurs. There are three separate triggers, based on any combination of the configurable pins (PIO) when selected as user I/O functions. You can also use a two-byte serial string to initiate a trigger.

Figure 4-14. E-mail Settings

```
**************** E-mail ******************
Mail server: 0.0.0.0
Unit       :
Domain     :
Recipient 1:
Recipient 2:

*** Trigger 1
Serial Sequence: 00,00
CP1: X
CP2: X
CP3: X
Message :
Priority: L
Min. notification interval: 1 s
Re-notification interval  : 0 s

*** Trigger 2
Serial Sequence: 00,00
CP1: X
CP2: X
CP3: X
Message :
Priority: L
Min. notification interval: 1 s
Re-notification interval  : 0 s

*** Trigger 3
Serial Sequence: 00,00
CP1: X
CP2: X
CP3: X
Message :
Priority: L
Min. notification interval: 1 s
Re-notification interval  : 0 s
```

E-mail Setup

E-mail setup requires you to set up the e-mail server location as follows:

Mail server	The IP address in decimal-dot notation.
Unit	The user name used by the XPort to send e-mail messages.
Domain	The domain name of your e-mail server.
Recipient 1	Full e-mail address of the recipient.
Recipient 2	Full e-mail address of the second recipient.

Trigger Setup

A trigger event can occur when the unit receives two bytes of a specified sequence on the serial port, or because of a specified combination of conditions on the configurable pins.

If the serial sequence is set to **00,00**, the trigger is disabled. At the **Serial Sequence** prompt, enter the ASCII Hex value. Example: A two byte sequence of 12 would be 0x31, 0x32.

If the configurable pins are all set to **X** (Don't Care), then they are disabled. If both the serial sequence and the configurable pins are disabled, the trigger is disabled.

Note: *You can set the configurable pins to A = Active, I = Inactive, or X = Don't Care. Active can mean Active Low or Active High. To change the configurable pins' settings, you must use DeviceInstaller or send setup records to Port 77FE.*

Message	The subject line of the e-mail.
Priority	L is for normal priority; H is for high priority.
Min. notification interval	The minimum time allowed between individual triggers. If a trigger event occurs faster than the minimum interval, the unit ignores the trigger.
Re-notification interval	If a single trigger event stays asserted, then the unit sends an e-mail message at this time interval.

Each trigger is independent of the others. Each condition within an individual trigger must be met before the unit will send the e-mail.

Expert Settings

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

Caution: *Only an expert should change these parameters. You must definitely know the consequences the changes might have.*

TCP Keepalive time in s (1s – 65s; 0s=disable) (45)

ARP Cache timeout in s (1s – 600s) (600)

TCP Keepalive time in seconds

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 drops that connection.

ARP Cache timeout in seconds

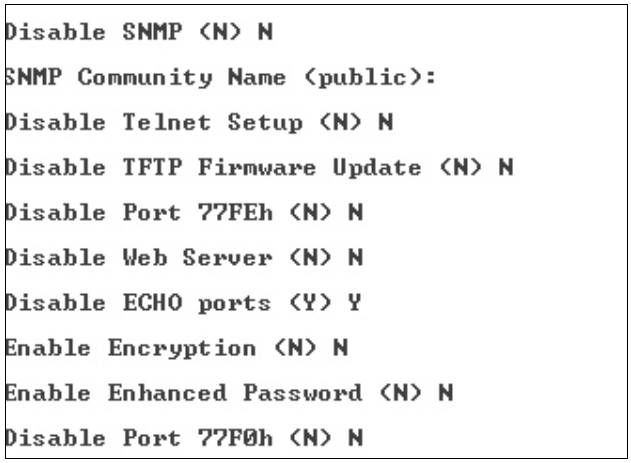
Whenever the unit communicates with another device on the network, it adds an entry into its ARP table. The ARP Cache timeout option allows you to define how many seconds (1-600) the unit will wait before timing out this table.

Security Settings

You can change security 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.

Caution: *Disabling both Telnet Setup **and** Port 77FE will prevent users from accessing the setup menu from the network.*

Figure 4-16. Security Settings



Disable SNMP

This setting allows you to disable the SNMP protocol on the unit for security reasons.

SNMP Community Name

This setting allows you to change the SNMP community name. Community name is a required field for NMS to read or write to a device. The default setting is **public**. The name is a string of 1 to 13 characters.

Disable Telnet Setup

Note: *If you choose to disable this option, keep in mind that disabling both Telnet Setup and Port 77FE will prevent users from accessing the setup menu from the network.*

This setting defaults to the N (No) option. The Y (Yes) option disables access to Setup Mode by Telnet (port 9999). It only allows access locally via the web pages and the serial port of the unit.

Disable TFTP Firmware Upgrade

This setting defaults to the N (No) option. The Y (Yes) option disables the use of TFTP to perform network firmware upgrades. With this option, you can download firmware upgrades over the serial port using DeviceInstaller's Recover Firmware procedure. (See Recovering the Firmware using the Serial Port on 6-2.)

Disable Port 77FE (Hex)

Note: *If you choose to disable this option, keep in mind that disabling both Telnet Setup and Port 77FE will prevent users from accessing the setup menu from the network.*

Port 77FE is a setting that allows DeviceInstaller, Web-Manager, and custom programs to configure the unit remotely. You may wish to disable this capability for security purposes.

The default setting is the N (No) option, which enables remote configuration. You can configure the unit by using DeviceInstaller, web pages, Telnet, or serial configuration.

The **Y** (Yes) option disables remote configuration and web sites.

Note: *The Y (Yes) option disables many of the GUI tools for configuring the unit, including the embedded Web-Manager tool.*

Disable Web Server

This setting defaults to the N (option). The Y (Yes) option disables the web server.

Disable ECHO Ports

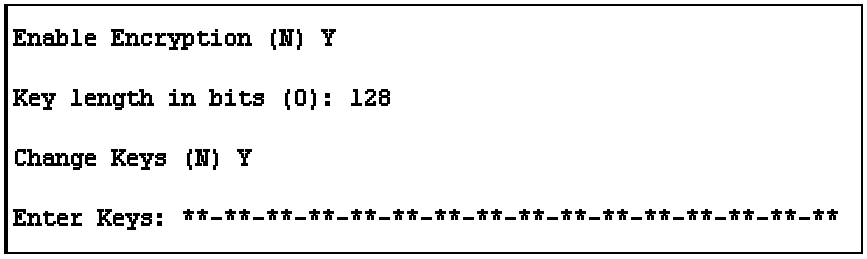
This setting controls whether the serial port echoes characters it receives.

Enable Encryption

This option displays **only** if you purchased the encrypted version of the Lantronix XPort. You can enable or disable (default) Rijndael encryption. Rijndael is the block cipher algorithm recently chosen by the National Institute of Science and Technology (NIST) as the Advanced Encryption Standard (AES) to be used by the US government.

To enable encryption, select the key length (128, 192 or 256 bits) and enter the encryption key in hexadecimals (32, 48, or 64, respectively). The hexadecimals are echoed as asterisks to prevent onlookers from seeing the key.

Figure 4-18. Encryption Keys



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

Generally, one of two situations applies.

- Encrypted XPort-to-XPort communication (and in the future, XPort communication to other Lantronix device servers) is supported without extra effort.
- The XPort 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 XPort. To ease the development process, Lantronix provides an AES encryption DLL for Windows and protocol source code samples. See the document entitled *Encryption*

Enabling Your Serial Device on the Lantronix web site (www.lantronix.com) for more instructions and sample code.

The following export agreement is required for the optional encryption:

I agree that I will not export or re-export this software file 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 software, 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.

Enable Enhanced Password

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

Disable Port 77F0 (Hex)

Port 77F0 is a setting that allows a custom application to query or set the three XPort configurable pins when they are functioning as general purpose I/O (GPIO). You may want to disable this capability for security purposes. The default setting is the N (No) option, which enables GPIO control. The Y (Yes) option disables the GPIO control interface.

Factory Defaults

Select **7** to reset the unit's Channel 1 configuration, e-mail settings, and expert settings to the factory default settings. The server configuration settings for IP address, gateway IP address, and netmask remain unchanged. The configurable pins' settings also remain unchanged. The specific settings that this option changes are listed below.

Channel 1 Configuration

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 for serial channel 1	0x0D (CR)
All other parameters	0

Expert Settings

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

Security Settings

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
Port 77F0h	Enabled

E-mail Settings

Priority	L
Min. notification interval	1 (second)
All other parameters	0 (e.g., e-mail notification and triggers are disabled)

Exit Configuration Mode

You have two options:

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

5: GPIO Interface

This chapter includes the following topics:

Configurable Pins

The XPort has three pins (CP1-3) that you can configure for General Purpose I/O (GPIO).

Note: *You can also configure the pins for serial port control lines, such as CTS, RTS, DTR, and DCD, and diagnostic outputs to LEDs, using DeviceInstaller.*

You can use these GPIO pins to control devices such as relays, servers, lights, monitor switches, sensors, and even processes such as data transfer.

You can set the functions for the three pins independently and in any combination. The initial directions (input/output) and active levels (active low or high) at boot up can also be configured through 77FE, for example, by using DeviceInstaller.

This chapter describes how the directions, active levels, and states can be dynamically controlled and probed through special port 77F0.

Features:

- TCP and UDP can be used.
- The protocol supports up to 32 GPIO for future products.
- Function configuration can be retrieved.
- Input or output selection can be retrieved and controlled.
- Active low or high selection can be retrieved and controlled.
- Active or inactive selection can be retrieved and controlled.
- 77F0 can be disabled.

Every change of state (active/inactive) requires a command over TCP or UDP, and thus is not very fast. If you use this port for data transfer, the throughput is low, usually up to 1Kbps.

Control Protocol

The GPIO control protocol is a simple, proprietary protocol, which is described below.

Guidelines

The GPIO control protocol is described from the PC side. *Send* means from PC to XPort. *Response* comes from XPort to PC.

The protocol allows for control of up to 32 GPIOs. How many are actually available depends on the product. XPort has only three.

The parameters are four bytes long and represent GPIOs 0-31, with GPIO0 in bit 0 of the first byte (Little Endian). Parameter bits for configurable pins not configured as GPIOs are undefined for **Get** commands and ignored on **Set** commands.

Every command consists of nine bytes: one command type of one byte and two parameters of four bytes each.

Command	Parameter 1				Parameter 2			
0	1	2	3	4	5	6	7	8

On some commands, one or all parameters are ignored.

For UDP, command type and parameters need to be in the same datagram.

Responses to valid commands are always five bytes long, consisting of the returned command byte and as parameters in the current or updated values. In case of an invalid command, only one byte with value 0FFh is returned.

Command	Parameter 1			
0	1	2	3	4

When sending a command (TCP and UDP), wait for the response before sending the next command.

Commands

Byte 0 Command Types

10h	**Get functions**
11h	**Get directions** (input or output)
12h	**Get active levels** (high active or low active)
13h	**Get current states** (active or not active)
19h	**Set directions**
1Ah	**Set active levels**
1Bh	**Set current states**

As you can, see there is no **Set functions** command. Since the pin's function depends on the hardware in which the XPort is embedded, that configuration is only allowed via 77FE. Settings changed by any of the **Set** commands are not stored and are lost when the unit is powered down or rebooted.

Command 10h, Get Functions

Send:

No parameters

Response:

1 parameter
Bytes 1-4: Functions
Bit X 1 means general purpose IO available to the user.
0 means dedicated function (e.g., serial flow control, diagnostics) for configurable pin X.

Command 11h, Get Directions

Send:

No parameters

Response:

1 parameter
Bytes 1-4: Directions
Bit X 1 means GPIO X is an output.
0 means it is an input.

Command 12h, Get Active Levels

Send:

No parameters

Response:

1 parameter
Bytes 1-4: Active levels
Bit X 1 means GPIO X is active low (0V when active, 3.3V when inactive).
0 means it is active high (3.3V when active, 0V when inactive).

Command 13h, Get Current States

Send:

No parameters

Response:

1 parameter
Bytes 1-4: States
Bit X 1 means GPIO X is active
0 means it is inactive.

Command 19h, Set Directions

Send:

2 parameters
Bytes 1-4: Mask
Bit X 1 means the direction for GPIO X will be updated with the value in the second parameter.
0 means the direction for that GPIO will not change.
Bytes 5-8: New Directions
Bit X 1 means GPIO X will become an output.
0 means it will become an input.

Response:

1 parameter
Bytes 1-4: The updated directions

Command 1Ah, Set Active Levels

Send:

2 parameters
Bytes 1-4: Mask
Bit X 1 means the direction for GPIO X will be updated with the value in the second parameter.
0 means the active type for that GPIO will not change.
Bytes 5-8: New Active Levels
Bit X 1 means GPIO X will become active low.
0 means it will become active high.

Response:

1 parameter
Bytes 1-4: Updated active levels

Command 1Bh, Set States

Send:

2 parameters
Bytes 1-4: Mask
Bit X 1 means the state for GPIO X will be updated with the value in the second parameter.
0 means the state for that GPIO will not change.
Bytes 5-8: New States
Bit X 1 means GPIO X will become active.
0 means it will become inactive.

Response:

1 parameter
Bytes 1-4: Updated states

Examples

Example 1: PC sends command 1 to find out which configurable pins are available as GPIO.

PC -> XPort: 10h, 00h, 00h, 00h, 00h, 00h, 00h, 00h, 00h
XPort -> PC: 10h, 03h, 00h, 00h, 00h

Command details:

10h = command 10h
00h, 00h, 00h, 00h = ignored
00h, 00h, 00h, 00h = ignored

Response details:

10h = response to command 10h
04h, 00h, 00h, 00h =

bits 0 and 1 are 0 →CP1 and CP2 are configured as GPIOs.
bit 2 is 1 → CP3 is configured as either serial control or diagnostics.
The other bits are ignored because there are only three configurable pins on the XPort.

Example 2: PC sends command 1Bh to change the current states of GPIO 0 and 1.

PC -> XPort: 1Bh, 01h, 00h, 00h, 00h, 00h, 00h, 00h, 00h
XPort -> PC: 1Bh, 05h, 00h, 00h, 00h

Command details:

1Bh = command 1Bh
01h, 00h, 00h, 00h = the mask that determines which GPIOs will be changed.

bit 0 is 1 → GPIO0 will be changed.
bit 1 is 0 → GPIO1 will remain the same.

00h, 00h, 00h, 00h = the new states

bit 0 is 0 → GPIO0 will become 0.
bit 1 is ignored since it is masked out.

Response details:

1Bh = response to command 1Bh
05h, 00h, 00h, 00h =

bit 0 is 1 → GPIO0 = 1
bit 1 is 0 → GPIO1 = 0
bit 2 is 1 → GPIO2 = 1
The other bits are ignored because there are only three configurable pins on the XPort.

6: Updating Firmware

This chapter explains how to obtain and update the unit's firmware. It includes the following topics:

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.lantronix.com).

Reloading Firmware

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

Here are *typical* names for those files. Check the Lantronix web site for the latest versions and release notes.

Table 6-1. Firmware Files

ROM File	COB
XPTE150.ROM	GENW3402.COB (Web-Manager)

Please refer to the DeviceInstaller User Guide for information about reloading firmware using DeviceInstaller. The other methods are discussed below:

Using TFTP

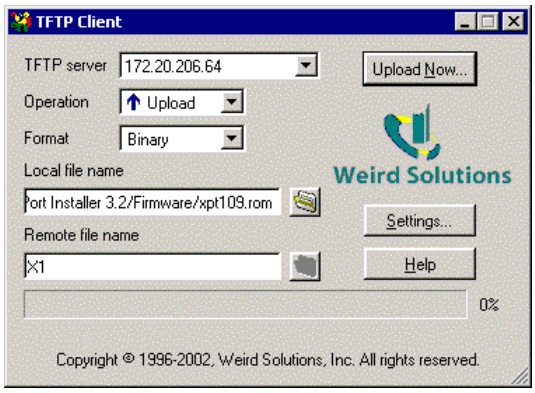
To download new firmware from a computer:

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

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

2. In the **TFTP server** field, enter the IP address of the unit being upgraded.
3. Select **Upload** operation and **Binary** format.
4. Enter the full path of the firmware file in the **Local file name** field.
5. In the **Remote file name** field, enter the **current** internal operational code or **WEB6** for the internal Web interface. (For XPort, **X1** = Standard Tunnel)
6. Click the **Upload Now** button to transfer the file to the unit.

Figure 6-2. TFTP Window



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

Recovering the Firmware using the Serial Port

If for some reason the firmware is damaged, you can recover the firmware file by using the serial port to download the *.ROM file.

1. Start DeviceInstaller. If your PC has more than one network adapter, a message displays. Select an adapter and click **OK**.
2. Click the **Search** icon to display the Lantronix device servers on your local network
3. Select the device server.
4. From the **Action** menu, select **Advanced/Recover Firmware**. The Recover Firmware window displays.
5. Enter the local port on your PC and the location of the firmware file. The **Device Model** should indicate XPort.
6. Click **OK** to download the file.

See also Recovering Firmware in the *DeviceInstaller User Guide*.

7: Monitoring the Network

Monitor Mode is a command-line interface used for diagnostic purposes.

This chapter includes the following topics:

There are two ways to enter Monitor Mode: locally via the serial port or remotely via the network.

Entering Monitor Mode via the Serial Port

To enter Monitor Mode locally:

1. Follow the same steps used for setting the serial configuration parameters (see Using the Serial Port on page 4-2).
2. Instead of typing three **x** keys, however:
   a) Type **zzz** (or **xx1**) to enter Monitor Mode with network connections.
   b) Type **yyy** (or **yyy**) to enter Monitor Mode without network connections.

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

Entering Monitor Mode via the Network Port

To enter Monitor Mode using a Telnet connection:

1. Establish a Telnet session to the configuration port (9999). The following message appears:

```
MAC address 00204A0113A3
Software version 01.0b9 (021219)  XPT
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 (xxx.xxx.xxx.xxx). If you enter the IP address, the command is applied to another unit with that IP address. If you do not enter the IP address, the command is executed locally.

Note: *All commands must be in capital letters.*

Table 7-1. Monitor Mode Commands

Command	Command Name	Function
VS x.x.x.x	Version	Queries software header record (16 bytes) 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 (120 bytes).
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.

Responses to some of the commands are given in Intel Hex format.

Note: *Entering any of the commands listed above generates one of the following command response codes:*

Table 7-4. 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

8: 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.

When troubleshooting the following problems, make sure that the XPort is powered up. Confirm that you are using a good network connection.

This chapter includes the following topics:

Problems and Error Messages

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 attempt to assign an IP address to the unit by the ARP method, the *Press Enter to go into Setup Mode error* (described below) message displays. Now when you Telnet to the device server, the connection fails.	When you Telnet to port 1 on the device server, you are only assigning a temporary IP address. When you Telnet into port 9999 and do not press **Enter** quickly, the device server reboots, causing it to lose the IP address.	Telnet back to 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 ***Press Enter to go into Setup Mode*** message 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 *Press Enter to go into Setup Mode* message.

Problem/Message	Reason	Solution
When you Telnet to port 1 to assign an IP address to the device server, 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.
	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 device server.
	The device server 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 device server 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. ***Note:*** *You cannot assign an IP address to a device server through a router*.
The device server is not communicating with the serial device it is attached to.	The most likely reason is the wrong serial settings were chosen.	The serial settings for the serial device and the device server must match. The default serial settings for the device server are RS-232, 9600 baud, 8 character bits, no parity, 1 stop bit, no flow control.
When you try to enter the setup mode on the device server via the serial port, you get no response.	The issue is most likely 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.
You can ping the device server, but not Telnet to the device server on port 9999.	There may be an IP address conflict on your network You are not Telnetting to port 9999. The Telnet configuration port (9999) is disabled within the device server security settings.	Turn the device server 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 device server). PING X.X.X.X (X.X.X.X is the IP of the device server). If you get a response, then there

Problem/Message	Reason	Solution
		is a duplicate IP address on the network. If you do not get a response, use the serial port to verify that Telnet is not disabled.
The device server appears to be set up correctly, but you are not communicating with your device attached to the device server across the network.	If you are sure that the serial port setting is correct, then you may not be connecting to the correct socket of the device server. Another possibility is that the device server 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 device server by checking the state of CP1, if it has been configured for LED1 functionality. If the state of CP1 is blinking consistently, or is completely off, then there is a good socket connection. If the state of CP1 is low, use the Connect Mode option **C0** for making a connection to the device server from the network. Use Connect Mode option **C1** or **C5** for a connection to the network from the device server. See the full list of Connect Mode options in Connect Mode on page 4-7.
When connecting to the Web-Manager within the device server, the *No Connection With The Device Server* message displays.	Your computer is not able to connect to port 30718 (77FEh) on the device server.	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 device server.

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:

- To check our online knowledge base or send a question to Technical Support, go to http://www.lantronix.com/support.
- 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) 89 31787 817
E-mail: eu_techsupp@lantronix.com or eu_support@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 model number
- Lantronix MAC number
- Software version (on the first screen shown when you Telnet to port 9999)
- Description of the problem
- Status of the unit when the problem occurred (please try to include information on user and network activity at the time of the problem).

9: IP Addresses

Each TCP/IP node on a network host has a unique IP address. This address provides the information needed to forward packets on the local network and across multiple networks if necessary.

IP addresses are specified as **x.x.x.x**, where each x is a number from 1 to 254; for example, 192.0.1.99. The unit must be assigned a unique IP address to use TCP/IP network functionality.

This chapter includes the following topics:

Components of the IP Address

Network Portion

The network portion of the IP address is determined by the network type: Class A, B, or C.

Table 9-1. .Network Portion of IP Address

Network Class	Network Portion of Address
Class A	First byte (2nd, 3rd, and 4th bytes are the host)
Class B	First 2 bytes (3rd and 4th bytes are the host)
Class C	First 3 bytes (4th byte is the host)

In most network examples, the host portion of the address is set to zero.

Table 9-4. Available IP Addresses

Class	Address Range	Comments
A	1.0.0.1 to 126.255.255.254	126 networks of 16,777,214 hosts
B	128.1.0.1 to 191.254.255.254	16,328 networks of 65,534 hosts
C	192.0.1.1 to	2,097,150 networks of 254 hosts

Class	Address Range	Comments
	223.255.254.254	
D	224.0.0.0 to 239.255.255.254	Reserved for multicast groups
E	240.0.0.0 to 254.255.255.254	Reserved for experimental and future use

Consider the IP address 36.1.3.4. This address is a Class A address; therefore, the network portion of the address is 36.0.0.0 and the host portion is 1.3.4.

Subnet Portion

The subnet portion of the IP address represents which *sub-network* the address is from. Sub-networks are formed when an IP network is broken down into smaller networks using a *subnet mask.*

A router is required between all networks and all sub-networks. Generally, hosts can send packets directly only to hosts on their own sub-network. All packets destined for other subnets are sent to a router on the local network.

Host Portion

The host portion of the IP address is a unique number assigned to identify the host.

Network Address

A host address with all host bits set to 0 addresses the network as a whole (as in routing entries), for example, 192.168.0.0.

Broadcast Address

A host address with all host bits set to 1 is the broadcast address (for every station), for example, 192.168.0.255.

You may *not* use a network or broadcast address as a host address; for example, 192.168.0.0 identifies the entire network, and 192.168.0.255 identifies the broadcast address.

IP Subnet Mask

An IP subnet mask divides an IP address differently from the standards defined by the classes A, B, and C. An IP subnet mask defines the number of bits to be taken from the IP address as the network or host sections. The unit prompts for the number of host bits to be entered and then calculates the netmask, which displays in standard decimal-dot notation (for example, 255.255.255.0) after you save the parameters.

Table 9-7. Standard IP Network Netmasks

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

Table 9-10. 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

Private IP Networks and the Internet

If your network is not and will not be connected to the Internet, you may use any IP address. If your network is connected or will be connected to the Internet, or if you intend to operate the unit on an intranet, use one of the reserved sub-networks. Consult your network administrator with questions about IP address assignment.

Network RFCs

For more information about IP addresses, refer to the following documents, which can be located on the World Wide Web using one of the following directories or indices:

RFC 950	Internet Standard Subnetting Procedure
RFC 1700	Assigned Numbers
RFC 1117	Internet Numbers
RFC 1597	Address Allocation for Private Networks

Alternative Ways to Assign an IP Address

In 3:Getting Started, we described how to assign an IP address using DeviceInstaller. This section covers other methods for assigning an IP address over the network.

Note: *You can also assign the IP address using a serial connection. (See Using the Serial Port on page 4-2.)*

DHCP

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

You can use the DeviceInstaller software to search the network for the IP address your unit has been assigned by the DHCP server and add it to the managed list.

Note: *This DHCP address does **not** appear in the unit's Setup Mode and Web-Manager 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 on page 7-1) 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. 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 it finds a DHCP server, 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.

ARP and Telnet

If the unit has no IP address, you can use Address Resolution Protocol (ARP) method from UNIX and Windows-based systems to assign a temporary IP address.

To assign a temporary IP address:

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 (on the product label on the bottom of the unit).

   ```
   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:

   ```
   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.

   telnet 191.12.3.77 1

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

   telnet 191.12.3.77 9999

Continue with Using Setup Mode on page 4-1.

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 configure the unit and store the changes permanently.*

A:Binary to Hex Conversions

Many of the Device Server'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.

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.

Binary to Hexadecimal Conversion Table

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

In 4:Using Setup Mode, the binary bit fields for options in connect mode, disconnect mode, flush mode, interface mode, and pack control mode are described in detail. The following pages are a summary of the possible hexadecimal entries for each of these options.

Connect Mode Options

Note: *Character response codes are C=connect, D=disconnect, N=unreachable*

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
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

Connect Mode Options

Accept Incoming Connections	Serial Response Upon Connection	Active Connection Startup	Hostlist	Hex
Never	None (quiet)	Manual connection	Hostlist	N/A
Never	None (quiet)	Autostart	Hostlist	25
Never	None (quiet)	UDP	Hostlist	
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
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:

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

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

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	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
	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

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
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

Flush Mode Options

Serial to Network Clear input buffer upon:	Network to Serial Clear output buffer upon:	Alternate Packing Algorithm	Hex
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
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

Flush Mode Options

Serial to Network Clear input buffer upon:	Network to Serial Clear output buffer upon:	Alternate Packing Algorithm	Hex
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
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

Flush Mode Options

Serial to Network Clear input buffer upon:	Network to Serial Clear output buffer upon:	Alternate Packing Algorithm	Hex
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
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

Flush Mode Options

Serial to Network Clear input buffer upon:	Network to Serial Clear output buffer upon:	Alternate Packing Algorithm	Hex
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
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

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

Pack Control Options

Pack Control Options

Sendcharacter Defined by a:	Trailing Characters	Packing Interval	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

Pack Control Options

Sendcharacter Defined by a:	Trailing Characters	Packing Interval	Send Immediately after Sendcharacter	Hex
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
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

B: Networking Terms

Address Space

A linear array of locations that a thread can access. Simple processors have only one, and these processors are referred to as `linear' addressing.

Auto-Negotiate

Clause 28 of the IEEE 802.3u standard specifies a MAC sub layer for the identification of the speed and duplex mode of connection being supported by a device. Support of this feature is optional for individual vendors.

Auto-Sense

Ability of a 10/100 Ethernet device to interpret the speed or duplex mode of the attached device and to adjust to that rate. Official term is Auto-Negotiation in Clause 28 of the IEEE 802.3u standard.

Baseband LAN

A LAN that uses a single carrier frequency over a single channel. Ethernet, Token Ring, and Arcnet LANs use baseband transmission.

Baud

Unit of signal frequency in signals per second. Not synonymous with bits per second since signals can represent more than one bit. Baud equals bits per second only when the signal represents a single bit.

Binaries

Binary, machine readable forms of programs that have been compiled or assembled. As opposed to Source language forms of programs.

Block

A block is a variable-size piece of memory that a task can acquire. Blocks are allocated from heaps. [Related: Buffer, heap]

BOOTP

A TCP/IP network protocol that lets network nodes request configuration information from a BOOTP "server" node.

bps

Bits per second, units of transmission speed.

Bridge

A networking device that connects two LANs and forwards or filters data packets between them based on their destination addresses. Bridges operate at the data link level (or MAC-layer) of the OSI reference model, and are transparent to protocols and to higher level devices like routers.

Bus

A LAN topology in which all the nodes are connected to a single cable. All nodes are considered equal and receive all transmissions on the medium.

Byte

A data unit of eight bits.

Channel

The data path between two nodes.

DHCP (Dynamic Host Configuration Protocol)

Short for Dynamic Host Configuration Protocol, a protocol for assigning dynamic IP addresses to devices on a network. With dynamic addressing, a device can have a different IP address every time it connects to the network. In some systems, the device's IP address can even change while it is still connected. DHCP also supports a mix of static and dynamic IP addresses.

Domain Name

A domain name is a text name appended to a host name to form a unique host name across internets.

Download

The transfer of a file or information from one network node to another. Generally refers to transferring a file from a "big" node, such as a computer, to a "small" node, such as a terminal server or printer.

End Node

A node such as a PC that can only send and receive information for its own use. It cannot route and forward information to another node.

Ethernet

The most popular LAN technology in use today. The IEEE standard 802.3 defines the rules for configuring an Ethernet network. It is a 10 Mbps, CSMA/CD baseband network that runs over thin coax, thick coax, twisted pair or fiber optic cable.

Firmware

Alterable programs in semipermanent storage, e.g., some type of read-only or flash reprogrammable memory.

Flash ROM

See ROM.

Framing

Dividing data for transmission into groups of bits, and adding a header and a check sequence to form a frame.

FTP

File Transfer Protocol, a TCP/IP protocol for file transfer.

Full-Duplex

Independent, simultaneous two-way transmission in both directions, as opposed to half-duplex transmission

Gateway

A device for interconnecting two or more dissimilar networks. It can translate all protocol levels from the Physical layer up through the Applications layer of the OSI model, and can therefore interconnect entities that differ in all details.

Hardware Address

See Network Address.

Host

Generally a node on a network that can be used interactively, i.e., logged into, like a computer.

Host Table

A list of TCP/IP hosts on the network along with their IP addresses.

IEEE 802.3

The IEEE (Institute of Electrical and Electronic Engineers) standard that defines the CSMA/CD media-access method and the physical and data-link layer specifications of a local area network. Among others, it includes 10BASE2, 10BASE5, 10BASE-FL, and 10BASE-T Ethernet implementations.

Internet

A series of interconnected local, regional, national and international networks, linked using TCP/IP. Internet links many government, university, and research sites. It provides E-mail, remote login and file transfer services.

Internetworking

General term used to describe the industry composed of products and technologies used to link networks together.

IP Address

See Network Address.

ISO Layered Model

The International Standards Organization (ISO) sets standards for computers and communications. Its Open Systems Interconnection (OSI) reference model specifies how dissimilar computing devices such as Network Interface Cards (NICs), bridges, and routers exchange data over a network. The model consists of seven layers. From lowest to highest, they are: Physical, Data Link, Network, Transport, Session, Presentation, and Application. Each layer performs services for the layer above it.

KB

Kilobyte. KBps is Kilobytes per second.

Kbps

Kilobits per second.

LAN

Local Area Network, a data communications system consisting of a group of interconnected computers, sharing applications, data, and peripherals. The geographical area is usually a building or group of buildings.

Latency

The delay incurred by a switching or bridging device between receiving the frame and forwarding the frame.

Layer

In networks, layers refer to software protocol levels comprising the architecture, with each layer performing functions for the layers above it.

Line Speed

Expressed in bps, the maximum rate at which data can reliably be transmitted over a line using given hardware.

Logical Link

A temporary connection between source and destination nodes, or between two processes on the same node.

Mbps

Megabits per second.

MIB

Management Information Base, a database of network parameters used by SNMP and CMIP (Common Management Information Protocol) to monitor and change network device settings. It provides a logical naming of all information resources on the network that are pertinent to the network's management.

Multicast

A multicast is a message that is sent out to multiple devices on the network by a host.

Name Server

Software that runs on network hosts charged with translating (or resolving) text-style names into numeric IP addresses.

Network

An interconnected system of computers that can communicate with each other and share files, data and resources.

Network Address

Every node on a network has one or more addresses associated with it, including at least one fixed hardware address such as "ae-34-2c-1d-69-f1" assigned by the device's manufacturer. Most nodes also have protocol specific addresses assigned by a network manager.

Network Management

Administrative services for managing a network, including configuring and tuning, maintaining network operation, monitoring network performance, and diagnosing network problems.

Node

Any intelligent device connected to the network. This includes terminal servers, host computers, and any other devices (such as printers and terminals) that are directly connected to the network. A node can be thought of as any device that has a "hardware address."

Open System Interconnect (OSI)

See "ISO."

Packet

A series of bits containing data and control information, including source and destination node addresses, formatted for transmission from one node to another.

Physical Address

An address identifying a single node.

Physical Layer

Layer 1, the bottom layer of the OSI model, is implemented by the physical channel. The Physical layer insulates Layer 2, the Data Link layer, from medium-dependent physical characteristics such as baseband, broadband, or fiber-optic transmission. Layer 1 defines the protocols that govern transmission media and signals.

Port

The physical connector on a device enabling the connection to be made.

Protocol

Any standard method of communicating over a network.

Remote Access

Access to network resources not located on the same physical Ethernet. (Physical Ethernet here refers to an entire site network topology.)

Router

Device capable of filtering/forwarding packets based upon data link layer information. Whereas a bridge or switch may only read MAC layer addresses to filter, routers are able to read data such as IP addresses and route accordingly.

RS-232 Signals

RXD Receive Data
TXD Transmit Data
RTS Ready to Send
CTS Clear to Send
DTR Data Terminal Ready
CD Carrier Detect
DSR Data Set Ready
RI Ring Indicator

Server

A computer that provides resources to be shared on the network, such as files (file server) or terminals (terminal server).

Session

A connection to a network service.

SNMP

Simple Network Management Protocol, allows a TCP/IP host running an SNMP application to query other nodes for network-related statistics and error conditions. The other hosts, which provide SNMP agents, respond to these queries and allow a single host to gather network statistics from many other network nodes.

Source Code

Programs in an uncompiled or unassembled form.

Switch

Multiport Ethernet device designed to increase network performance by allowing only essential traffic on the attached individual Ethernet segments. Packets are filtered or forwarded based upon their source and destination addresses.

TCP/IP

Transmission Control Protocol (TCP) and Internet Protocol (IP) are the standard network protocols in UNIX environments. They are usually implemented, used together, and called TCP/IP.

Telnet

Telnet is an application that provides a terminal interface between hosts using the TCP/IP network protocol. It has been standardized so that Telnetting to any host should give one an interactive terminal session, regardless of the remote host type or operating system. Note that this is very different from the LAT software, which allows only local network access to LAT hosts only.

10Base-T

Ethernet running on unshielded twisted pair (UTP) cable. Note that 10BASE-T is a point-to-point network media, with one end of the cable typically going to a repeater/hub and the other to the network device.

100Base-TX

Specifies 100-Mbps operation using the CSMA/CD protocol over two pairs of category 5 UTP cable.

Terminal Server

A concentrator that facilitates communication between hosts and terminals.

TFTP

Trivial File Transfer Protocol. On computers that run the TCP/IP networking software, TFTP is used to quickly send files across the network with fewer security features than FTP.

Throughput

The amount of data transmitted between two points in a given amount of time, e.g., 10 Mbps.

Topology

The arrangement of the nodes and connecting hardware that comprises the network. Types include ring, bus, star, and tree.

Twisted-Pair Cable

Inexpensive, multiple-conductor cable comprised of one or more pairs of 18 to 24 gauge copper strands. The strands are twisted to improve protection against electromagnetic and radio frequency interference. The cable, which may be either shielded or unshielded, is used in low-speed communications, as telephone cable. It is used only in baseband networks because of its narrow bandwidth.

UTP

Unshielded twisted pair, one or more cable pairs surrounded by insulation. UTP is commonly used as telephone wire.

Wide Area Network (WAN)

A network using common carrier transmission services for transmission of data over a large geographical area.