ARTISAN®
TECHNOLOGY GROUP

Your **definitive** source for quality pre-owned equipment.

Artisan Technology Group
(217) 352-9330 | sales@artisantg.com | artisantg.com

Full-service, independent repair center
with experienced engineers and technicians on staff.

We buy your excess, underutilized, and idle equipment
along with credit for buybacks and trade-ins.

Custom engineering
so your equipment works exactly as you specify.

- Critical and expedited services
- In stock / Ready-to-ship
- Leasing / Rentals / Demos
- ITAR-certified secure asset solutions

Expert team | Trust guarantee | 100% satisfaction

All trademarks, brand names, and brands appearing herein are the property of their respective owners.

Find the *Lantronix CoBox-E2-01* at our website: *Click HERE*

LANTRONIX®

CoBox-FL/CoBox-FL-IAP
User Guide



Part Number 900-285

Revision E 8/03

Copyright and Trademark

© 2003, Lantronix. All rights reserved. No part of the contents of this book may be transmitted or reproduced in any form or by any means without the written permission of Lantronix. Printed in the United States of America.

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

Lantronix

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

Technical Support

Phone: 800-422-7044 or 9949-453-7198
Fax: 949-450-7226
On-line: www.lantronix.com/support

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.

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

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

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

Date	Rev.	Comments
07/01/01	C	Current release.
09/25/02	D	Revised for Device Installer, new format. Includes all CoBox-FL devices.
08/25/03	E	Updated warranty information.

Declaration of Conformity

(according to ISO/IEC Guide 22 and BS 7514)

Manufacturer's Name & Address:

Lantronix, 15353 Barranca Parkway, Irvine, CA 92618 USA

Declares that the following product:

Product Name Model: CoBox-FL/CoBox-FL-IAP Device Server

Conforms to the following standards or other normative documents:

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

Electromagnetic Emissions:

FCC Part 15, Subpart B, Class A
EN55022: 1998 (CISPR 22, Class A: 1993, A1: 1995, A2: 1996)
IEC 1000-3-2/A14: 2000
IEC 1000-3-3: 1994

Electromagnetic Immunity:

EN55024: 1998 Information Technology Equipment-Immunity Characteristics
IEC61000-4-2: 1995 Electro-Static Discharge Test
IEC61000-4-3: 1996 Radiated Immunity Field Test
IEC61000-4-4: 1995 Electrical Fast Transient Test
IEC61000-4-5: 1995 Power Supply Surge Test
IEC61000-4-6: 1996 Conducted Immunity Test
IEC61000-4-8: 1993 Magnetic Field Test
IEC61000-4-11: 1994 Voltage Dips & Interrupts Test
(L.V.D. Directive 73/23/EEC)

Supplementary Information:

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

Manufacturer's Contact:

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

Warranty

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

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

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

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

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

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

Sales Offices

The Americas
15353 Barranca Parkway
Irvine, CA 92618, USA
Phone: (949) 450-7227
Fax: (949) 450-7231
sales@lantronix.com

France
2 Rue Hélène Boucher
78280 Guyancourt
France
Tel: +33 1 39 30 41 74
Fax: +33 1 39 30 41 73
europesud@lantronix.com

Germany
Karlstrasse 49
78054 VS-Schwenningen
Germany
Tel: +49 (0)77 20 30 1620
Fax: +49 (0)77 20 30 1688
ursula.koch@lantronix.com

Asia Pacific
16th Floor
Cheung Kong Center
2 Queen's Road Central
Hong Kong
Tel: +852 2297 2287
Fax: +852 2297 2357
asiapacsales@lantronix.com

EMEA Sales
(Europe, Mid East, Africa)
eu_sales@lantronix.com
eu_order@lantronix.com

EMEA Technical Support
+49 (0) 7720 3016 20/57
eu_techsupp@lantronix.com

Table of Contents

1. Introduction 1-1
1.1 CoBox-FL 1-1
1.2 CoBox-FL-IAP Device Server 1-2
1.2.1 Industrial Automation Protocols 1-3
1.3 Network Protocols 1-4
1.3.1 Packing Algorithm 1-4
1.3.2 IP Address 1-4
1.3.3 Port Number 1-4
1.4 Serial Interface 1-5
1.4.1 Channel 1 1-5
1.4.2 Channel 2 1-6
1.5 RJ-45 Ethernet Interface 1-6
1.6 RJ-45 Ethernet Connector 1-7
1.7 ST-Fiber Ethernet Connectors 1-7
1.8 Serial Interface Cable 1-8
1.9 Network LEDs 1-8
1.10 Serial LEDs 1-9
1.11 Dimensions 1-10
1.12 Product Information Label 1-10
1.13 Software Support 1-10
1.14 Power Requirements 1-11
1.15 Technical Specifications 1-12

2. Getting Started 2-1
2.1 Addresses and Port Number 2-1
2.1.1 Ethernet (MAC) Address 2-1
2.1.2 Internet Protocol (IP) Address 2-1
2.1.3 Port Number 2-2
2.2 Physically Connecting the Unit 2-2
2.3 Methods of Assigning the IP Address 2-3
2.3.1 DHCP 2-4
2.3.2 AutoIP 2-4
2.4 DeviceInstaller 2-5
2.4.1 Install DeviceInstaller Software 2-5

2.4.2 Assign IP Address and Network Class 2-6
2.4.3 Test the IP Address 2-7
2.4.4 Add the Unit to the Manage List 2-8
2.4.5 Opening a Configuration Window 2-10
2.5 ARP and Telnet 2-11
2.6 Serial Port Login 2-12

3. Configuring the Unit 3-1
3.1 Configuring via Web Browser 3-1
3.2 Using DeviceInstaller 3-2
3.3 Web Manager Page 3-4
3.3.1 Unit Configuration 3-5
3.3.2 Server Properties 3-6
3.3.3 Port Properties 3-7
3.3.4 Technical Support 3-9
3.3.5 Update Settings 3-9
3.4 Configuring via the Setup Mode Window 3-10
3.4.1 Using a Telnet Connection 3-10
3.4.2 Using the Serial Port 3-12
3.5 Server Configuration (Network Configuration) 3-12
3.5.1 IP Address 3-12
3.5.2 Set Gateway IP Address 3-12
3.5.3 Netmask: Number of Bits for Host Part 3-13
3.5.4 Change Telnet configuration password 3-14
3.5.5 DHCP Naming 3-14
3.6 Channel 1 Configuration (Serial Port Parameters) 3-15
3.6.1 Baudrate 3-15
3.6.2 I/F (Interface) Mode 3-15
3.6.3 Flow 3-16
3.6.4 Port Number 3-16
3.6.5 Connect Mode 3-17
3.6.6 Remote IP Address 3-20
3.6.7 Remote Port 3-20
3.6.8 DisConnMode 3-20
3.6.9 Flush Mode (Buffer Flushing) 3-21
3.6.10 Pack Control 3-22
3.6.11 DisConnTime (Inactivity Timeout) 3-23
3.6.12 Send Characters 3-23
3.6.13 Telnet Terminal Type 3-23
3.6.14 Channel (Port) Password 3-23
3.7 Expert Settings 3-24
3.7.1 TCP Keepalive time in s 3-24

3.8 Security Settings 3-24
3.8.1 Disable SNMP 3-24
3.8.2 SNMP Community Name 3-24
3.8.3 Disable Telnet Setup 3-25
3.8.4 Disable TFTP Firmware Upgrade 3-25
3.8.5 Disable Port 77FE (Hex) 3-25
3.8.6 Disable Web Server 3-25
3.8.7 Enable Enhanced Password 3-25
3.9 Factory Defaults 3-25
3.10 Exit Configuration Mode 3-26
3.11 Get Configuration 3-26
3.12 Set Configuration 3-27

4. Updating Protocol (Firmware) 4-1
4.1 Protocol Firmware 4-1
4.2 Reloading Protocol Firmware 4-1
4.2.1 Via DeviceInstaller 4-2
4.2.2 Via TFTP 4-4
4.2.3 Via Another Unit 4-5
4.2.4 Via the Serial Port 4-6

5. DeviceComm Manager 5-1
5.1 Installing DeviceComm Manager 5-2
5.1.1 Install DeviceComm Manager 5-2
5.1.2 Setup 5-3

6. Troubleshooting 6-1
6.1 Technical Support 6-1
6.1.1 Technical Support 6-1

7. Monitor Mode 7-1
7.1 Monitor Mode 7-1
7.1.1 Entering Monitor Mode Via the Serial Port 7-1
7.1.2 Entering Monitor Mode Via the Network Port 7-1
7.1.3 Monitor Mode Commands 7-1

8. Network Configuration using UDP 8-1
8.1 UDP Datagrams 8-1
8.2 Configuring Multiple Devices 8-3
8.2.1 Acquiring a Valid Setup Record 8-3
8.2.2 Sending a Setup Record 8-4
8.2.3 The Intel Hex Format 8-5
8.2.4 Calculating the Checksum 8-6
8.2.5 Calculating the Two's Complement 8-6

8.3 Setup Records....8-7
8.3.1 Channel Parameters....8-8
8.3.2 Interface Mode....8-9
8.3.3 Baud Rate....8-10
8.3.4 Flow Control....8-10
8.3.5 Connect Mode....8-11
8.3.6 Disconnect Mode....8-12
8.3.7 Flush Mode (Buffer Flushing)....8-13
8.3.8 Pack Control....8-13
8.4 IP Addresses....8-14
8.4.1 Network Portion....8-14
8.4.2 Subnet Portion....8-14
8.4.3 Host Portion....8-15
8.4.4 Network Address....8-15
8.4.5 Broadcast Address....8-15
8.4.6 Private IP Networks and the Internet....8-16
8.4.7 Network RFCs....8-16

9. Binary to Hex Conversion....9-1
9.1 Connect Mode Options....9-1
9.2 Disconnect Mode Options....9-5
9.3 Flush Mode (Buffer Flushing) Options....9-7
9.4 Interface Mode Options....9-13
9.5 Pack Control Options....9-14

10. IP Addresses....10-1
10.1 Class A Network....10-1
10.2 Class B Network....10-1
10.3 Class C Network....10-1
10.4 Network Address....10-2
10.5 Broadcast Address....10-2
10.6 IP Netmask....10-2
10.7 Private IP Networks and the Internet....10-3
10.8 Network RFCs....10-3

11. Glossary....11-1

List of Figures

Figure 1 – CoBox-FL-IAP 1-2
Figure 2 - RJ-45 Connector 1-7
Figure 3 – CoBox-FL Connected to Serial Device and Network 2-2
Figure 4 – CD Main Window 2-5
Figure 5 - DeviceInstaller Window 2-6
Figure 6 - Assign IP Address Window 2-6
Figure 7 - Ping Device Window 2-7
Figure 8 - Search Network Window 2-8
Figure 9 - Devices in a Group 2-9
Figure 10 - Device Management Window 2-10
Figure 11 - Lantronix Web-Manager 3-4
Figure 12 - Server Properties Configuration on the Web Browser 3-6
Figure 13 - Setup Mode Window 3-11
Figure 14 - Device Installer 4-2
Figure 15 - Search Network Window 4-3
Figure 16 - Devices in a Group 4-3
Figure 17 - Upgrade Firmware 4-4
Figure 18 - TFTP Dialog Box 4-5
Figure 19 – UDS/CoBox Main Window 5-2
Figure 20 - Sample Setup Record in Intel Hex Format 8-3

List of Tables

Table 1 - Ethernet Interface Signals 1-7
Table 2 - CoBox-FL LED Functions 1-9
Table 3 - Technical Specs 1-12
Table 4 - Standard IP Network Netmasks 3-13
Table 5 - Netmask Examples 3-13
Table 6 - Interface Mode Options 3-15
Table 7 - Common Interface Mode Settings 3-16
Table 8 - Flow Control Options 3-16
Table 9 - Connect Mode Options 3-17
Table 10 - Manual Connection Address Example 3-18
Table 11 - Modem Mode Commands 3-19
Table 12 - Disconnect Mode Options 3-20
Table 13 - Flush Mode Options 3-21
Table 14 - Pack Control Options 3-22
Table 15 - Protocol Firmware 4-1
Table 16 - Problems and Error Messages 6-2
Table 17 - Monitor Mode Commands 7-2
Table 18 -Command Response Codes 7-2
Table 19 - UDP Configuration 8-1
Table 20 - Block Types 8-5
Table 21 - Setup Record Construction 8-7
Table 22 - Channel Parameters 8-8
Table 23 - Interface Mode Options 8-9
Table 24 - Common Interface Mode Settings 8-9
Table 25 - Baud Rate Settings 8-10
Table 26 - Flow Control Options 8-10
Table 27 - Connect Mode Options 8-11
Table 28 - Disconnect Mode Options 8-12
Table 29 - Flush Mode Options 8-13
Table 30 - Pack Control Options 8-13
Table 31 - Network Portion of IP Address 8-14
Table 32 - Available IP Addresses 8-14
Table 33 - Standard IP Network Netmasks 8-15
Table 34 - Netmask Examples 8-16
Table 35 - Binary to Hexadecimal Conversion Table 9-1
Table 36 - Connect Mode Options 9-2
Table 37 - Connect Mode Options for Modem Emulation 9-4

Table 38 - Disconnect Mode Options 9-5
Table 39 - Flush Mode Options 9-7
Table 40 - Interface Mode Options 9-13
Table 41 - Pack Control Options 9-14

1. Introduction

This manual describes the CoBox-FL family of Device Servers, including the CoBox-FL Device Server and the CoBox-FL-IAP Device Server with Industrial Automation Protocols.

Most of the material in this manual applies to all of the CoBox-FL products. However, in some cases there will be some features that apply to only one product. In those cases, a note will explain the variation.

Note: In most cases CoBox-FL refers to CoBox-FL and CoBox-FL-IAP.

1.1 CoBox-FL

The CoBox-FL Device Server connects serial devices to Ethernet networks using the IP protocol family (TCP for connection-oriented stream applications and UDP for datagram applications). A few of the different types of serial devices supported are listed below:

- Time/Attendance Clocks and Terminals
- 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

The CoBox-FL connects these devices through a TCP data channel or through a Telnet connection to computers or another Device Server. Datagrams can be sent by UDP.





The CoBox-FL supports RS-232, RS-422/485 through the DB-25F Channel 1 serial port. It supports RS-232 through the DB-9M Channel 2 serial port. It supports 10Mb/s Ethernet through an RJ-45 connector and through ST-Fiber connectors. It can be configured via HTTP, SNMP, DHCP or Telnet. It contains a Flash ROM for easy software upgrades.

1.2 CoBox-FL-IAP Device Server

Note: This section is for the CoBox-FL-IAP only.

The Lantronix Industrial Automation Platform (IAP) family of Device Servers allows a single network and protocol to connect multiple serial devices from many vendors. IAP provides the automation industry with a network-enabling solution using TCP/IP and standard Ethernet networks that is vendor-independent.

By encapsulating serial data and transporting it over Ethernet, the Device Server allows virtual serial links to be established over Ethernet and IP (TCP/IP, UDP/IP) networks. As a result, limited distance, point-to-point, direct serial connections can be extended within the plant, throughout the facility, or across the global enterprise. The following picture is one of the Device Servers in the IAP family.



Figure 1 – CoBox-FL-IAP

Lantronix provides IAP Device Servers specifically designed for different industrial environments.

- CoBox-DR1-IAP, with a DIN rail interface for harsh environments or alongside controls instruments in electrical panels.
- CoBox-FL-IAP, with fiber connectivity for long cable runs or electrically hazardous environments.
- UDS-10-IAP, a compact Device Server for use in less demanding environments.

A few examples of attached devices are:

- PLCs
- AC/DC drives
- CNC systems
- Operator panels and message displays
- Process Controls
- Instrumentation
- Power monitoring equipment
- Scales and weighing systems
- Barcode scanners
- Label printers
- Most factory floor serial devices

1.2.1 Industrial Automation Protocols

IAP Device Servers, adapted to multiple factory environments, can unite any mixture of equipment from industrial automation vendors into a single reliable pipeline. This new and open infrastructure opens the way for data to flow in real time from all your plant devices up to your IT layer.

IAP Device Servers are delivered with IAP Standard Tunneling protocol and can be loaded with industrial communication protocols. The suite of protocols include DF1 (Rockwell Automation) and Modbus (Schneider Electric). Where the IAP Standard Tunneling protocol is limited to exclusive, standard ASCII device-to-device connections, the industrial protocols offer connections to other devices that require special formatting or features simultaneously.

For information about using any of the industrial communication protocols, see the user manuals on the software CD or our web site. Protocol firmware files are also contained on the CD and new versions are available from the Lantronix web site.

You can set up the unit using the serial port, or remotely over Ethernet using Telnet or a web browser. The CD that comes with your Device Server includes DeviceInstaller, a Windows based configuration software that simplifies the process of installing protocols and configuring them for use with attached devices. IAP Device Servers use Flash memory for maintenance-free, non-volatile storage which allows for fast system upgrades.

1.3 Network Protocols

Note: CoBox-FL refers to CoBox-FL and CoBox-FL-IAP except where noted.

The CoBox-FL uses TCP/IP protocols for network communication. The supported standards are: ARP, UDP, TCP, ICMP, Telnet, TFTP, DHCP, AutoIP, and SNMP. For transparent connections, TCP/IP (binary stream) or Telnet protocols are used. Firmware upgrades can be made with the TFTP protocol.

The IP (Internet Protocol) protocol defines addressing, routing, and data-block handling over the network. The TCP (transmission control protocol) assures that no data is lost or duplicated, and that everything sent into the connection on one side arrives at the target exactly as it was sent.

For typical datagram applications where devices interact with others without maintaining a point-to-point connection, UDP datagram is used.

1.3.1 Packing Algorithm

The two available packet algorithms (which define how and when packets are sent to the network) are software selectable. The standard algorithm is optimized for applications where CoBox-FL is used in a local environment, allowing for very small delays for single characters while trying to keep the packet count low. The alternate packing algorithm minimizes the packet count on the network and is especially useful for applications in routed Wide Area Networks. Various parameters can be set in this mode to economize the serial data stream.

1.3.2 IP Address

Every active device connected to the TCP/IP network must have a unique IP address. This IP address is used to reference a specific device, for example, to build a connection to CoBox-FL's serial port. See Appendix A for a complete description of IP Addressing.

1.3.3 Port Number

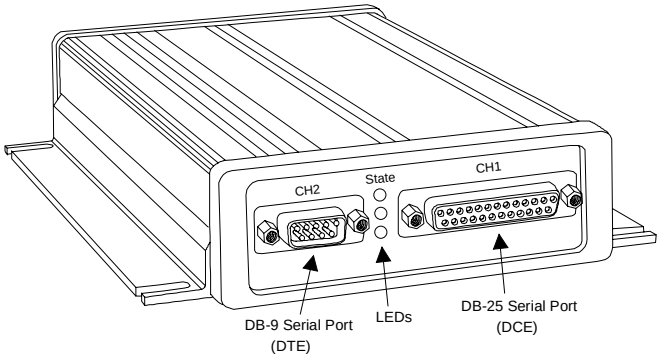
A destination IP address and a port number define every TCP connection and every UDP datagram. A port number is necessary to address an application or a channel on a network host. The port number can be compared to an extension on a PBX system.

A Telnet application (login to a host with an ASCII terminal) is commonly assigned TCP port number 23. More than one Telnet connection can be established to one host using the Telnet port; however, the other peer IP address/port number combinations must be different.

In the CoBox-FL, a port number can be configured on the channel (port). The CoBox-FL uses this port number for outgoing messages and incoming connections, or UDP datagrams, which are addressed to its port number. Port 9999 (decimal) is used for remote configuration.

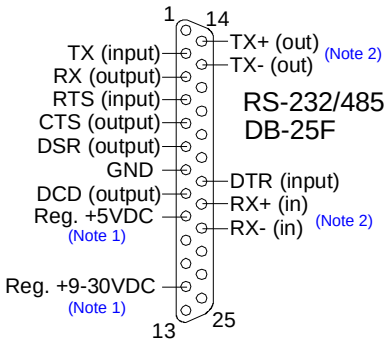
1.4 Serial Interface

The CoBox-FL has two serial ports. CH 1 uses a DB-25F (DCE) connector and supports RS-232, RS-422/485. CH 2 uses a DB-9 connector and supports RS-232 only. It supports 10Mb/s Ethernet through the RJ-45 (10BASE-T) connector or the ST-Fiber (10BASE-FL). It can be configured via HTTP, SNMP, DHCP or Telnet. It contains a Flash ROM for easy software upgrades.



1.4.1 Channel 1

The CoBox-FL Channel 1 is a female DB-25F supporting RS-232C, RS-485, or RS-422 DCE serial interface. The default serial port settings are 9600 baud, 8 data bits, no parity, and 1 stop bit.



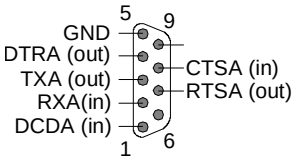
Note 1: The Device Server can alternately be powered up via the serial port using one of these pins.

Note 2: The minus sign (-) is sometimes shown as A (TXA), and the plus sign is sometimes shown as B (TXB)

For RS-485 2-wire functionality, connect pin 14 to 21, and connect pin 15 to 22.

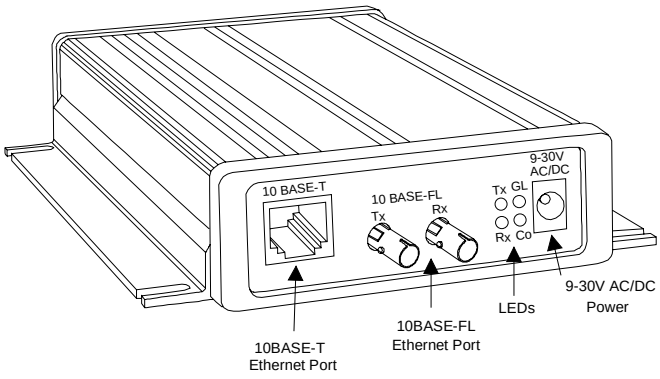
1.4.2 Channel 2

The CoBox-FL Channel 2 is a male DB-9M supporting RS-232C DTE serial interface.



1.5 RJ-45 Ethernet Interface

The CoBox-FL's back panel contains a 9-30V AC/DC power plug, four LEDs, an ST-Fiber (10BASE-FL) Ethernet port, and an RJ-45 (10BASE-T) Ethernet port. Both Ethernet ports support 10 Mbps and are auto detecting.



Note: Do not attempt to connect both Ethernet ports simultaneously. If one is used, the other is disabled.

1.6 RJ-45 Ethernet Connector

The next drawing shows a typical RJ-45 connector. The color is not standard but very typical of an Ethernet Patch cable. Pin 1 is located at the top of the connector (Orange + White). The view is from the end of the connector.

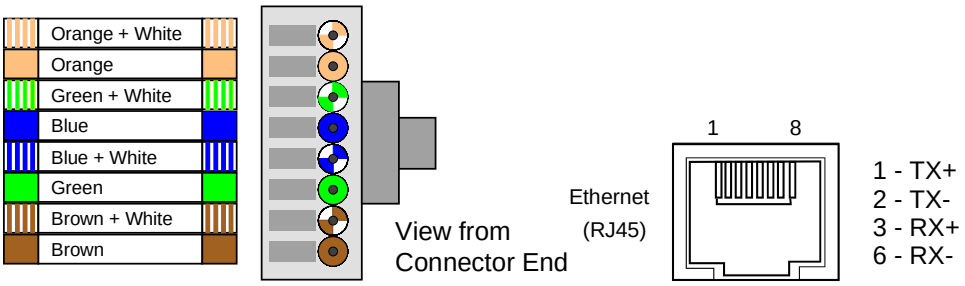
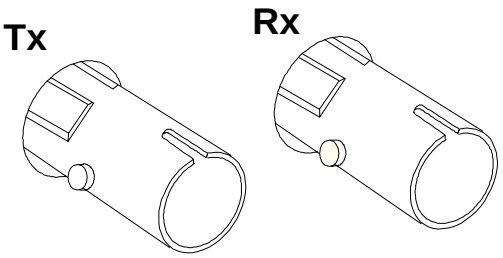


Figure 2 - RJ-45 Connector

Table 1 - Ethernet Interface Signals

Signal Name	DIR	PIN	Primary Function
TX+	Out	1	Transmit Data +
TX-	Out	2	Transmit Data -
RX+	In	3	Differential Ethernet Receive Data +
RX-	In	6	Differential Ethernet Receive Data -

1.7 ST-Fiber Ethernet Connectors

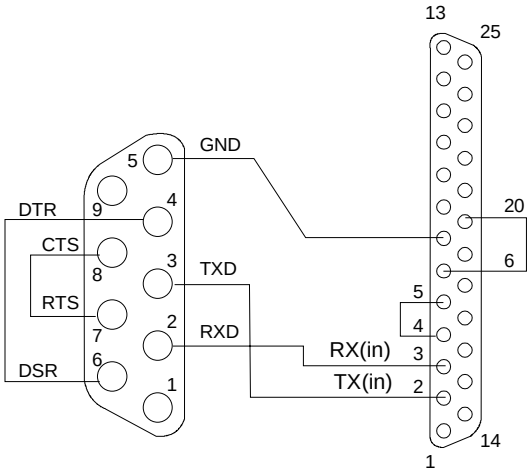


The CoBox-FL also supports 10Mbit Ethernet through an ST-Fiber Ethernet connector.

Note: Do not attempt to connect both Ethernet ports simultaneously. If one is used, the other is disabled.

1.8 Serial Interface Cable

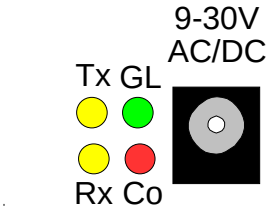
The CoBox-FL can be connected to a serial or Ethernet device for setup and configuration. The serial device can be RS-232 or RS-485/422. The following diagram shows a typical interface cable for the RS-232 Serial interface. The UDS-M-SBC is an optional male DB-25 to RS-485 screw block connector.



DTE, 9-Pin, FEMALE DCE, 25-Pin, MALE

1.9 Network LEDs

The following table explains the function of the four network LEDs.



LED	Meaning
GL (Good Link)	Lights solid green to indicate network port is connected to the network.
Tx (Network Transmit)	Blinks yellow to indicate network packets are transmitting.
Rx (Network Receive)	Blinks yellow to indicate network packets are receiving.
Co (Collision)	Blinks red to indicate network collisions.

1.10 Serial LEDs

Simultaneously lit red and green LEDs means something is wrong. If the red LED is lit or blinking, count the number of times the green LED blinks between its pauses. Blink patterns indicate which fault condition exists. The following table explains the functions of the three serial LEDs.

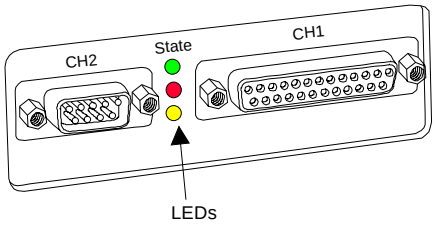


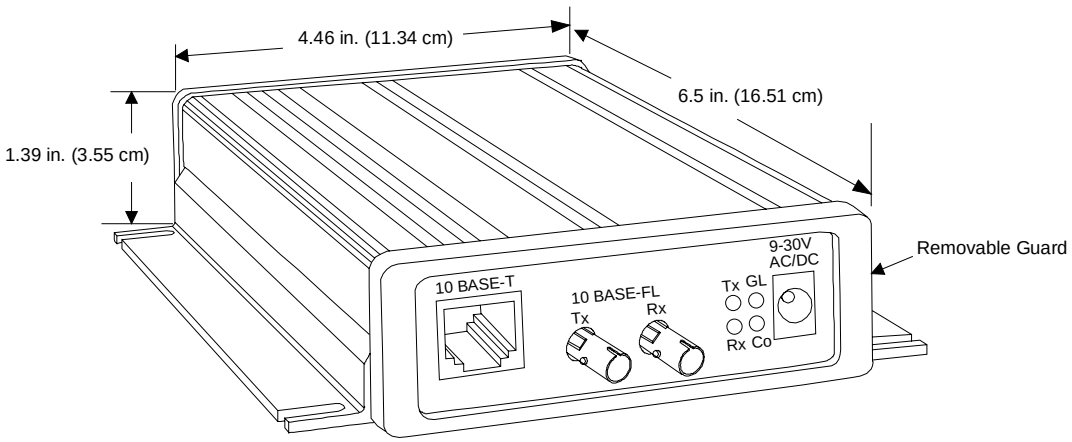
Table 2 - CoBox-FL LED Functions

LED	Meaning
GREEN CH1	Lights solid green to indicate that Channel 1 does not have a connection to or from the network. Blinks green to indicate that Channel 1 does have a connection to or from the network.
YELLOW CH2	Lights solid yellow to indicate Channel 2 does not have a connection to or from the network. Blinks yellow to indicate Channel 2 does have a connection to or from the network.
RED Diagnostic	Blinks or lights solid red in combination with the green (Channel 1) LED to indicate diagnostics and error detection. Red solid, green (Channel 1) blinking: 1x: EPROM checksum error 2x: RAM error 3x: Token Ring error 4x: EEPROM checksum error 5x: Duplicated IP address on the network Red blinking, green (Channel 1) blinking: 4x: Faulty network connection 5x: No DHCP response received

1.11 Dimensions

The CoBox-FL dimensions are shown in the following drawing.

Note: For CoBox-FL and CoBox-FL-IAP.



1.12 Product Information Label

The product information label contains important information about your specific unit.



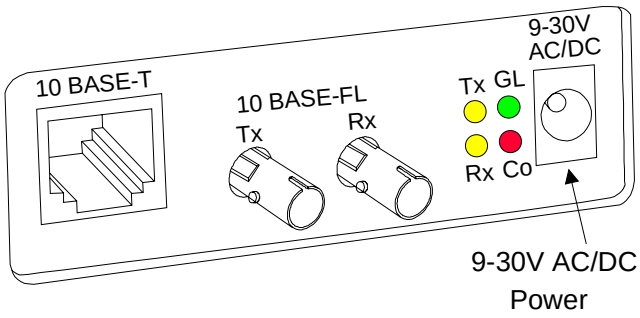
1.13 Software Support

DeviceInstaller is a powerful software utility for configuring device servers from a network connection. For more information, see *Using DeviceInstaller* on page 3-2.

Lantronix DeviceComm Manager is a Windows based COM port redirector software utility. Its function is to redirect customer application data destined for a local serial (COM) port to the PC's network port. Rather than going out the local port, the data is transmitted across the Ethernet network port using the TCP/IP protocol. For more information, see *DeviceComm Manager* on page 5-1.

1.14 Power Requirements

The CoBox-FL is shipped with a 12VDC, 0.8A, 100-240VAC, 50-60Hz power supply, but any power supply between 9VAC/DC and 30V AC/DC can be used.



1.15 Technical Specifications

Table 3 - Technical Specs

Category	Description
CPU, Memory	AMD 188ES CPU, 20MHz clock, 128kByte RAM
Flash, EPROM	512kByte Flash PROM
Installable Serial Protocols	Standard Tunnel (CoBox-FL, and CoBox-FL-IAP), Modbus (CoBox-FL-IAP), DF1 (CoBox-FL-IAP)
Serial Interface	DB-25F, RS-232C or RS-422/485 (DCE pinout) DB-9M, RS-232C (DTE pinout) Baud Rate selectable from 300bps to 115Kbps
Power Supply	External adapter for 9-30V AC/DC, 3 Watts Max
Dimensions	16.51 cm (6.5 in) , 11.34 cm (4.46 in) , 3.55 cm (1.39 in)
Weight	.48 kg (1.10 lbs)
Temperature	Operating range: 5° to +50° C (41to122° F) Max temperature change per hour: 20° C (36° F) Storage range: -40° to +66° C (-40 to 151° F)
Humidity	10% to 90% RH, non-condensing, 40% to 60% recommended
Case	Metal case with mounting flanges.
Protocols Supported	Auto IP, ARP, UDP/IP, TCP/IP, Telnet, ICMP, SNMP, DHCP, BOOTP, TFTP, and HTTP
Network Interface	RJ-45 10BASE-T or ST-Fiber 10BASE-FL
Serial Line Formats	Characters: 7 or 8 data bits Stop bits: 1,2 Parity: odd, even, none
Modem Control	DTR, DCD, CTS, RTS, DSR
Flow Control	CTS/RTS (hardware) XON/XOFF (software)
Management	Internal web server (Standard Tunneling only) SNMP (read only) Serial login Telnet login
System Software	Windows® 95/98/ME/NT/2000 based configuration software
LEDs	Network Transmit, Network Receive, Good Link, Collisions, Channel 1 Status, Channel 2 Status, Diagnostic
Compatibility	Ethernet: Version 2.0/IEEE 802.3

2. Getting Started

This section describes all the procedures for configuring your unit. For a short version, see the Quick Start Guide. Go to the Lantronix web site for the latest firmware and release notes.

CoBox-FL comes with Standard Tunnel Protocol and the CoBox-FL-IAP comes with the IAP Standard Tunnel Protocol. Both versions are similar but cannot be interchanged. Standard Tunneling is a serial communications protocol used by most Lantronix Device Servers. It can be configured to Ethernet-enable most serial devices such as barcode scanners, weigh scales, operator panels, data access devices, alpha numeric displays, and thousands of intelligent serial devices. For CoBox-FL-IAP users, see *Industrial Automation Protocols* on page 1-3

Loading industrial protocols to a CoBox-FL-IAP, such as IAP Modbus Bridge, may remove the web pages and change the configure dialogs. See the user manuals on individual protocols for protocol specific settings and configuration dialogs. Protocol manuals are found on the software CD. This section describes the setup and configuration dialogs for the Standard Tunnel Protocol.

Note: The following information is based on the condition that a CoBox-FL is loaded with Standard Tunnel Protocol. The CoBox-FL-IAP with IAP Standard Tunnel Protocol may have different options available.

2.1 Addresses and Port Number

2.1.1 Ethernet (MAC) Address

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

```
00-20-4A-21-18-17 or 00:20:4A:21:18:17
```

2.1.2 Internet Protocol (IP) Address

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

2.1.3 Port Number

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

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

2.2 Physically Connecting the Unit

The following diagram shows a typical hardware configuration for the CoBox-FL. Use one of the cables described in *Serial Interface Cable* on page 1-8 to connect a PC COM port to the CoBox-FL.

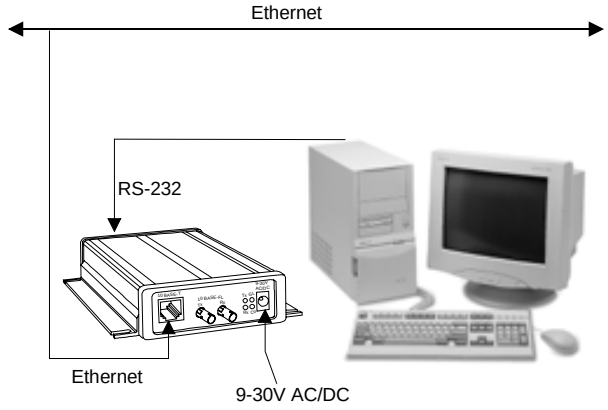


Figure 3 – CoBox-FL Connected to Serial Device and Network

1. Connect a serial device to your unit. See *Serial Interface Cable* on page 1-8 for more information about cable and connector specifications.
2. Connect an Ethernet cable to one of the Ethernet ports.
3. Supply power to your unit using a 9-30V AC/DC source.

Note: The required input voltage is 9-30V AC/DC (3 W maximum).

4. Supply power to the serial device.

Note: Connecting a device to an active Ethernet network can disrupt communications on the network. Make sure the device is configured for your application before connecting to an active network.

2.3 Methods of Assigning the IP Address

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

Method	Description
DHCP	A DHCP server automatically assigns the IP address and network settings. See *DHCP* on page 2-4.
DeviceInstaller **(Recommended)**	You manually assign the IP address using a graphical user interface (GUI) on a PC attached to a network. See *DeviceInstaller* on page 2-5.
ARP and Telnet	You manually assign the IP address and other network settings at a command prompt using a UNIX or Windows-based system. Only one person at a time can be logged into the configuration port (port 9999). This eliminates the possibility of several people simultaneously attempting to configure the unit. See *ARP and Telnet* on page 2-11.
AutoIP	This automatic method is appropriate when you have a small group of hosts rather than a large network. This method allows the hosts to negotiate with each other and assign addresses, in effect creating a small network. See *AutoIP* on page 2-4.
Serial Port Login	You initially configure the unit through a serial connection. See *Serial Port Login* on page 2-12.

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

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

IP Address: ___ ___ ___ ___
Subnet Mask: ___ ___ ___ ___
Gateway: ___ ___ ___ ___

2.3.1 DHCP

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

Provided a DHCP server exists on the network, it will assign the unit an IP address, gateway address, and subnet mask when the unit boots up. The CoBox-FL has acquired an IP address if the red LED stops flashing and the green GL LED is on continuously. (If no DHCP server exists, the unit responds with a diagnostic error: the red Diagnostic LED blinks continuously, and the green GL LED blinks five times. This blinking only continues for about 5 seconds.)

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

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

2.3.2 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 169.254.255.254) has been explicitly reserved for AutoIP-enabled devices. The range of Auto IP addresses is not to be used over the Internet.

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

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

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

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

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

2.4 DeviceInstaller

You can manually assign the IP address using DeviceInstaller software, which is found on the product CD. If you want to use a serial connection instead of an Ethernet connection to configure the device, go to *Serial Port Login* on page 2-12.

2.4.1 Install DeviceInstaller Software

1. Insert the product CD into your CD-ROM drive. The CD will automatically start and display the main window.

   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, deviceinstaller.exe (e.g., E:\deviceinstaller.exe).

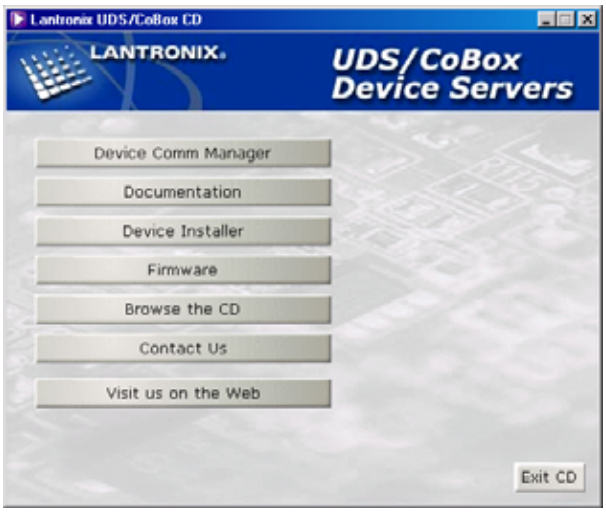


Figure 4 – CD Main Window

2. Click the **Device Installer** button. The installation wizard window displays.
3. Respond to the installation wizard prompts. (When prompted to select an installation type, select Typical.)

2.4.2 Assign IP Address and Network Class

Click the Start button on the Task Bar and select **Programs\Device Installer\Device Installer**. The Device Installer window displays.

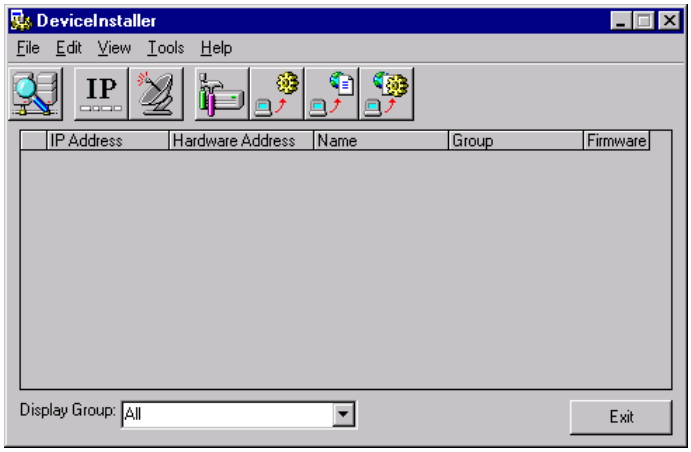


Figure 5 - DeviceInstaller Window

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

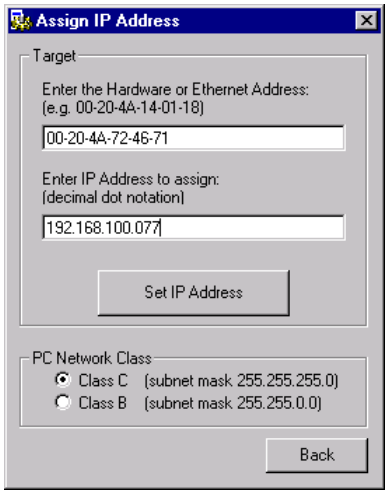


Figure 6 - Assign IP Address Window

2. In the **Enter the Hardware or Ethernet Address** field, enter the Ethernet address (MAC address), which is listed on the label on the side of the unit.

3. In the **Enter IP Address to assign** field, enter the unit's IP address in XXX.XXX.XXX.XXX format.
4. In the PC Network Class section, select the class (subnet mask). (Most users select Class C).
5. Click the **Set IP Address** button. (IP is assigned, pinged, and tested)
6. Confirm that the "Assign IP successful" message displays and click OK.
7. Click the **Back** button to return to the DeviceInstaller window.

2.4.3 Test the IP Address

1. Click the **Ping** icon . The Ping Device window displays.

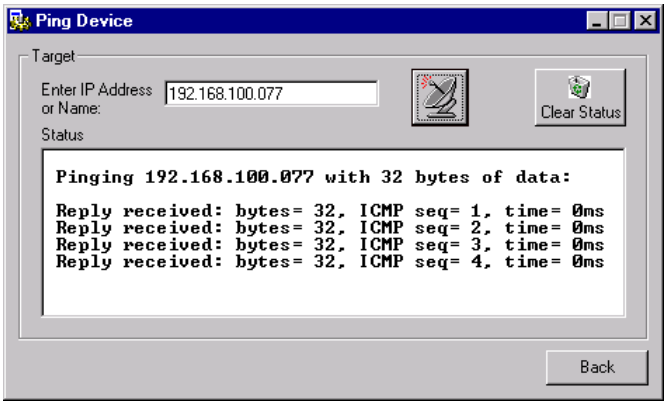


Figure 7 - Ping Device Window

2. Confirm that "Reply received" messages display in the window, indicating that the IP address has been entered successfully.

Note: If you do not receive "Reply received" 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. If you are not sure, check with your systems administrator.

3. Click the Back button to return to the Device Installer window.

2.4.4 Add the Unit to the Manage List

Now add the unit to the list of similar Lantronix devices on the network so that you can manage and configure it.

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

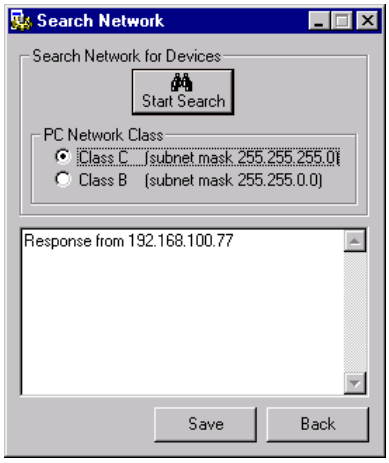


Figure 8 - Search Network Window

2. Select the PC Network Class. Class C is the default.
3. Click the **Start Search** button. A list of all active units displays.
4. Click the **Save** button. A confirmation message displays.
5. Click **OK**.

6. Click the **Back** button to return to the DeviceInstaller window. The DeviceInstaller window now lists all of the devices in the group, including the unit you are setting up. The hardware address and firmware release number for the unit display.

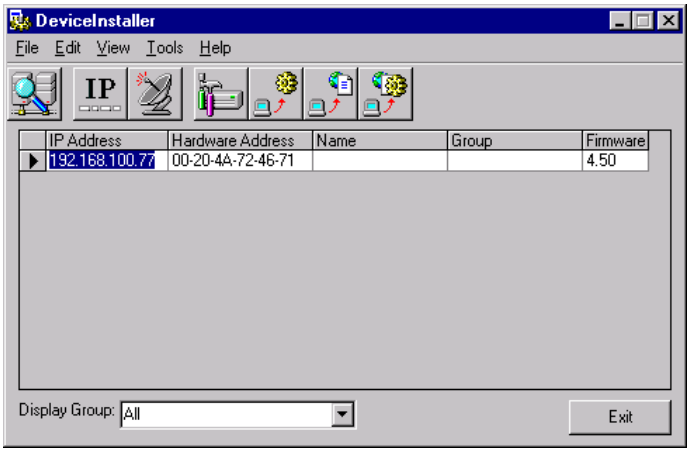


Figure 9 - Devices in a Group

Now you can manage (configure) the unit so that it works with the serial device on the network.

2.4.5 Opening a Configuration Window

1. Click the **Manage** icon . The Device Management window displays.

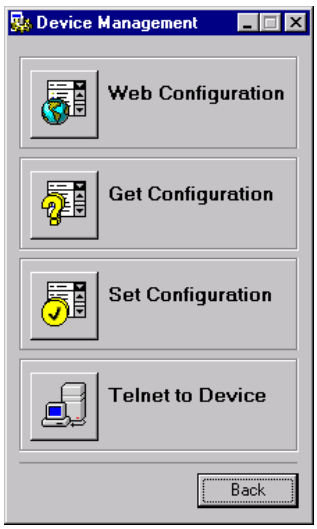


Figure 10 - Device Management Window

2. Do ***one*** of the following:

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

- To configure the unit via a Web browser, click the **Web Configuration** icon . The Lantronix Web-Manager window displays in your browser. For Web Configuration, see *Web Manager Page* on page 3-4.

- To configure the unit via a Telnet session, click the **Telnet to Device** icon . The Setup Mode window displays. For Telnet Configuration, see *Using a Telnet Connection* on page 3-10

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

*Note: The **Get Configuration** icon on the Device Management window allows you to save a configuration locally on your computer as a file. The **Set Configuration** icon sends a saved file to the unit.*

To **Get Configuration** information see *Get Configuration* on page 3-26. To **Set Configuration** of a specific device see *Set Configuration* on page 3-27.

2.5 ARP and Telnet

The unit's IP address must be configured before a network connection is available. You are able to ARP an address into a CoBox/UDS device even if there is already an address in the unit. 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. If you want to initially configure the unit through the network, follow these steps:

1. On a UNIX or Windows-based host, create an entry in the host's ARP table using the intended IP address and the hardware address of the unit, which is found on the product label on the bottom of the unit. Some UNIX hosts use colons ":" between hardware octets, and some use dashes "-". All Windows hosts use dashes.

   ```
   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 three seconds to go into Setup Mode. If you wait longer than three seconds, the unit will reboot and you will need to perform step 3 again.

   ```
   telnet 191.12.3.77 9999
   ```

5. Set all required parameters

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

2.6 Serial Port Login

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

1. Connect a console terminal or PC running a terminal emulation program to 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, cycle the unit's power (power off and back on). After power-up, the self-test begins and the red Diagnostic LED starts blinking. **You have one second** to enter three lowercase x characters.

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

3. At this point, the screen display is the same as when you use a Telnet connection. To continue with a serial port login, go to *Using a Telnet Connection* on page 3-10.

3. Configuring the Unit

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

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

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

Note: The configuration menus in this section show a typical device and all of the possible configuration options. Your device may have different configuration options.

3.1 Configuring via Web Browser

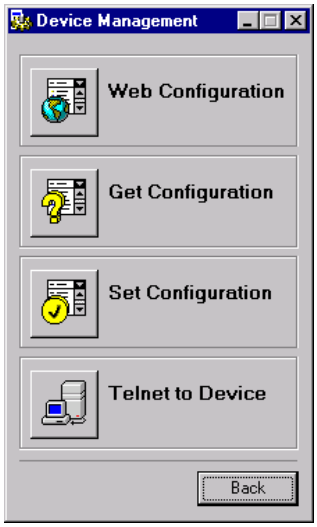
Open your JAVA enabled web browser and enter the IP address. The Lantronix Web Manager page will display. Go to *Web Manager Page* for a summary of the menu selections.

Note: The CoBox-FL-IAP may not have a web page or may use a different format web page.

3.2 Using DeviceInstaller

DeviceInstaller is a powerful software utility for configuring device servers from a network connection. This section uses the utility to demonstrate the various methods of configuring a device. The Device Management window is a common page for gaining access to different menus.

1. Start DeviceInstaller. Click the **Search for network for devices** icon . The Search Network window displays.
2. Click the **Start Search** button. A list of all active units displays.
3. Click the **Save** button. Click **OK** for the confirmation message. Click the **Back** button.
4. Click the **Manage device configuration** icon  to open the Device Management window.



5. For Web configuration, click the **Web Configuration** icon to start your browser. (A small Web Configuration window appears, showing the IP address.)

Go to *Web Manager Page* on page 3-4 for a summary of the menu selections.

Note: If your unit already has an IP address (see Methods of Assigning the IP Address), you can log into it using a standard Web browser that is Java enabled. Type the unit's IP address into the Web browser's URL (Address/Location) field.

6. For Telnet configuration, click the **Telnet to Device** icon. A small Telnet to Device window appears, showing the IP Address and the Port address. The main Lantronix Universal Device Server window opens.

Go to *Using a Telnet Connection* on page 3-10 for a summary of the menu selections.

7. To Get device configuration information see *Get Configuration* on page 3-26.

Configuration information can be read from a device and saved in a file.

8. To Set the configuration of a specific device see *Set Configuration* on page 3-27

A device can be configured by reading a configuration file and sending the information to the device.

3.3 Web Manager Page

Note: The CoBox-FL-IAP may not have a web page or may use a different format web page.

You can start a web browser for configuration by opening your JAVA enabled web browser and entering the IP address or by clicking the Web Configuration button on the Device Management window. The Lantronix Web Manager page will display.

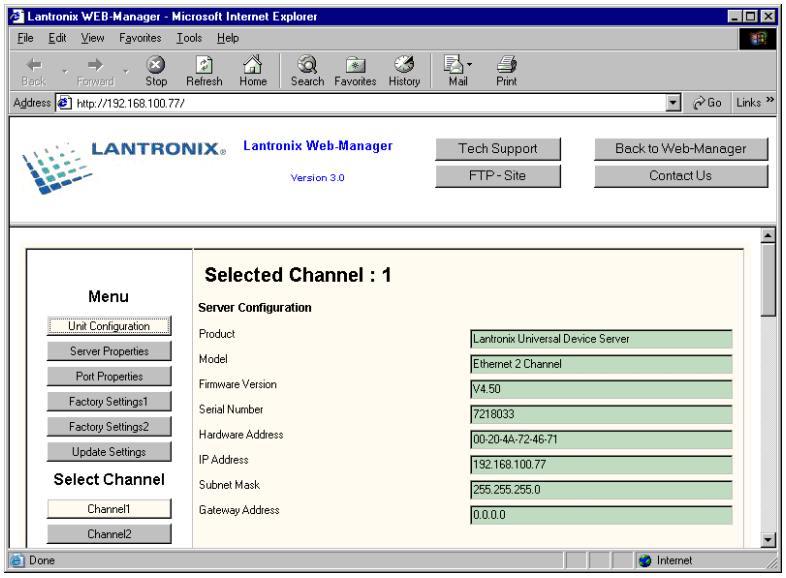


Figure 11 - Lantronix Web-Manager

Web Manager 3.0 has the following buttons:

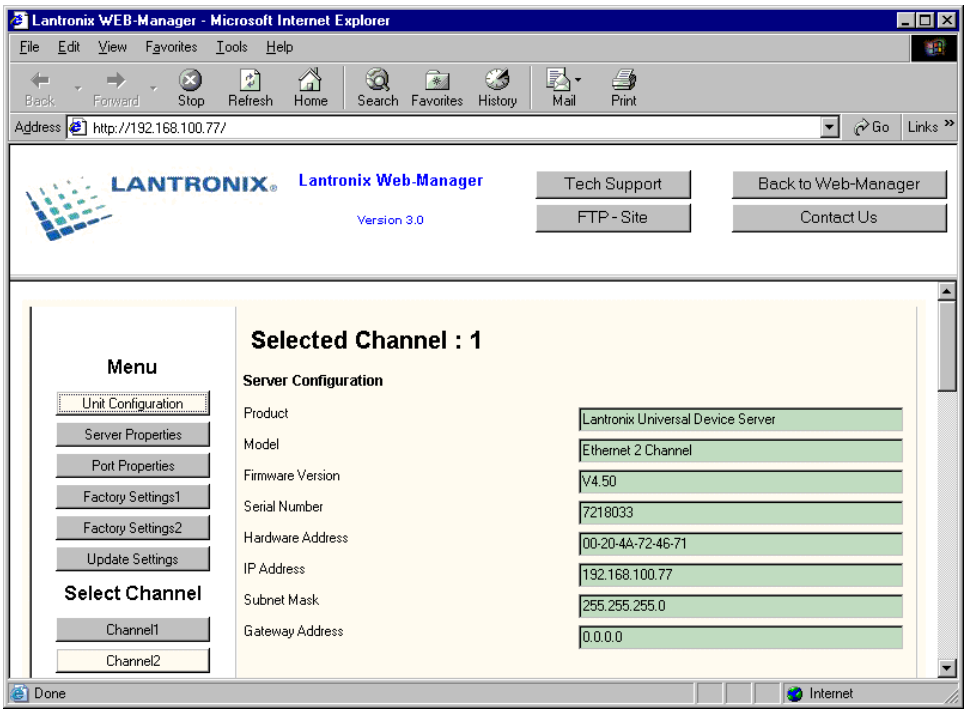
- Unit Configuration
- Server Properties
- Port Properties
- Factory Settings1 (also Factory Settings2 for devices with two serial channels)
- Update Settings
- Channel 1 (also Channel 2 for devices with two serial channels)
- Tech Support
- FTP – Site
- Back to Web-Manager
- Contact Us

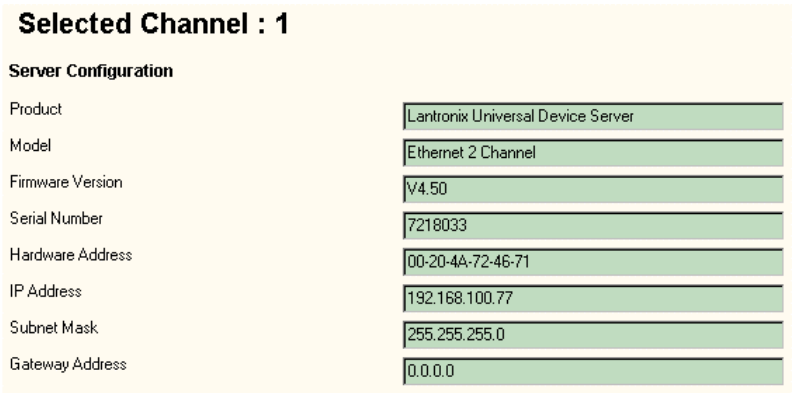
1. Use the menu (pushbuttons) to navigate to sub pages where you can configure server settings. See explanations of the configuration parameters later in this chapter.
2. When you are finished, click the **Update Settings** button to save your settings.

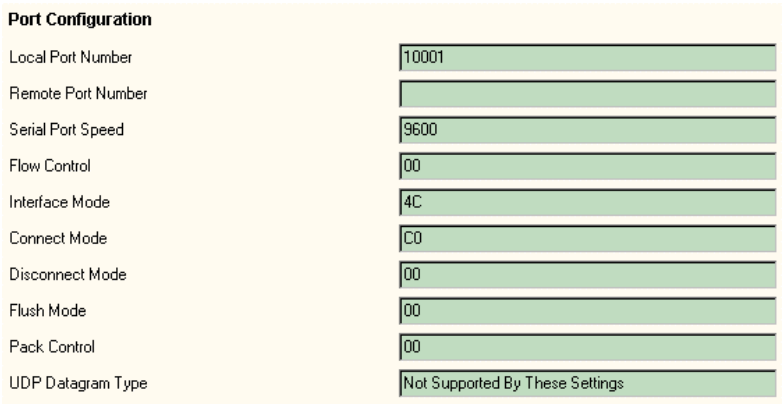
3.3.1 Unit Configuration

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

Note: The following screen shots represent the web page shown when the device is loaded with cbxw300.cob firmware.







3.3.2 Server Properties

You can change the server properties by editing any of the fields. Lingering over one of the fields will display operator messages. Changing the IP address will require you to enter the new IP address in the browser to reload the page.

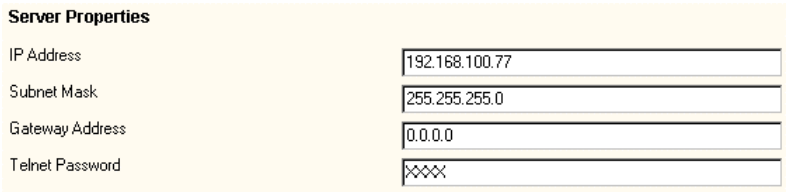


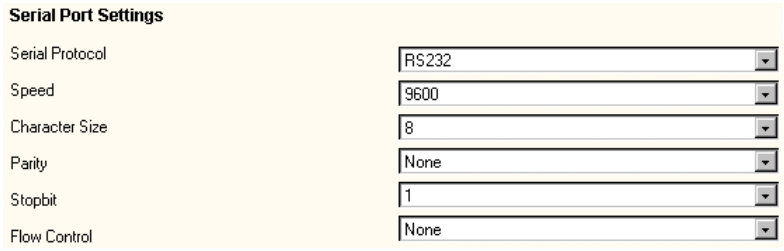
Figure 12 - Server Properties Configuration on the Web Browser

Telnet Password

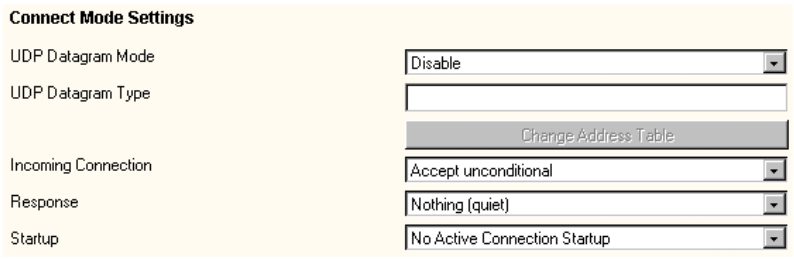
In the Telnet Password field, enter a password to prevent unauthorized access to the Setup Mode via a Telnet connection to port 9999. The password is limited to 4 characters. (An enhanced password setting of 16 characters is available under Security Settings on the Telnet Setup Mode window.)

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

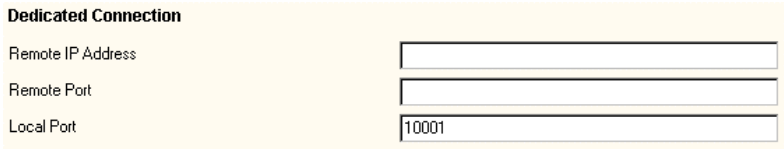
3.3.3 Port Properties



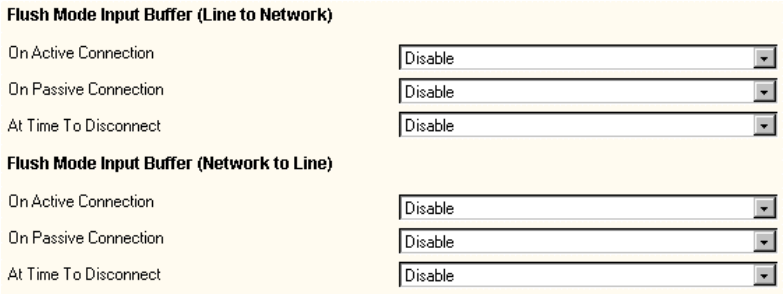
Serial Protocol: RS232, RS422/485 4-wire, RS485 2-wire
Speed: 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200
Character Size: 8, 7
Parity: None, Even, Odd
Stop Bit: 1,2
Flow Control: None, XON/XOFF, XON/XOFF Pass Characters to Host, CTS/RTS (Hardware)



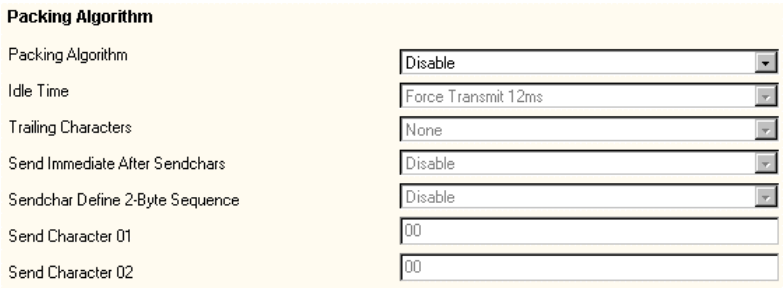
UDP Datagram Mode: Enable, Disable
UDP Datagram Type: (User selectable)
Incoming Connection: Accept unconditional, Accept Incoming/DTR (Inactive), Never accept incoming
Response: Nothing (quiet), Character response
Startup: No active startup, with any character, with active DTR (Inactive), with CR (0x0D) only, Manual Connection, Autostart, Modem Mode



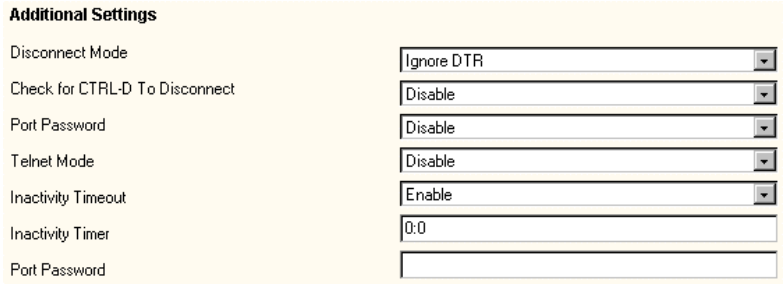
Remote IP Address: (user selectable)
Remote Port: (user selectable)
Local Port: 10001 (default 10001, user selectable)



On Active Connection: Enable, Disable
On Passive Connection: Enable, Disable
At Time of Disconnect: Enable, Disable



Packing Algorithm: Enable, Disable
Idle Time: Force transmit 12 ms, Force transmit 52 ms, Force Transmit 250 ms, Force Transmit 5000 ms
Trailing Characters: None, One, Two
Send Immediate After Sendchars: Enable, Disable
Send Define2-Byte Sequence: Enable, Disable
Send Character 01: (User Selectable)
Send Character 02: (User Selectable)



Disconnect Mode: with DTR Drop, Ignore DTR
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)

3.3.4 Technical Support

Several buttons provide direct links to Technical Support functions. You can use the **Tech Support** button to link directly to the Lantronix Tech Support web page, the **FTP-Site** button will link you to the web page for downloading new firmware, manuals, and other files. The **Contact Us** button will link you to the Contact Information page.

3.3.5 Update Settings

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

3.4 Configuring via the Setup Mode Window

3.4.1 Using a Telnet Connection

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

*Note: If you use the **Telnet to Device** icon on the Device Installer Device Management window **OR** a serial port login to establish the connection, skip steps 1and 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**.
3. The **Lantronix Universal Device Server** window displays.

```
 *** Lantronix Universal Device Server ***
Serial Number 7218033 MAC address 00:20:4A:72:46:71
Software version 04.5 (011025)

Press Enter to go into Setup Mode
```

4. To enter the Setup Mode, **you must press Enter within 5 seconds**. The configuration settings will appear. See *Figure 13 - Setup Mode Window.*

Note: The following line appears only with IAP Standard Tunnel Protocol Firmware.

```
Model: Device Server Plus+!  (Firmware Code: AQ)
```

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

```
*** basic parameters
Hardware: Ethernet Autodetect
IP addr – 0.0.0.0/DHCP/BOOTP/AutoIP, no gateway set
DHCP device name : not set

***************** Security *****************
SNMP is              enabled (not IAP firmware)
SNMP Community Name:         (not IAP firmware)
Telnet Setup is      enabled
TFPT Download is     enabled
Port 77Feh is        enabled
Web Server is        enabled
Enhanced password is disabled

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

***************** Expert ******************
TCP Keepalive : 0s           (not IAP firmware)

Change Setup  :0 Server configuration
               1 Channel 1 configuration
               5 Expert settings (not IAP firmware)
               6 Security
               7 Factory defaults
               8 Exit without save
               9 Save and exit                Your choice ?
```

Figure 13 - Setup Mode Window

3.4.2 Using the Serial Port

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

8. 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.
9. To enter Setup Mode, cycle the unit's power (power off and back on). After power-up, the self-test begins and the red Diagnostic LED starts blinking. **You have one second** to enter three lowercase **x** characters (**xxx**).

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

10. At this point, the screen display is the same as when you use a Telnet connection. To continue with a serial port login, go to *Using a Telnet Connection* on page 3-10.

3.5 Server Configuration (Network Configuration)

These are the unit's basic network parameters. The following parameters are displayed when you select **Server configuration**.

```
IP Address : (000) .(000) .(000) .(000)
Set Gateway IP Address (N)
Netmask: Number of Bits for Host Part (0=default)  (00)
Change telnet config password (N)
```

3.5.1 IP Address

The IP address must be set to a unique value in your network. See *Methods of Assigning the IP Address* on page 2-3 for more information about IP addressing.

3.5.2 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.

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

Table 4 - Standard IP Network Netmasks

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

Table 5 - 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

3.5.4 Change Telnet configuration password

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

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

3.5.5 DHCP Naming

There are 3 methods for assigning DHCP names to these products.

1) 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 will default 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.

2) Custom DHCP name. You can create your own DHCP name on these products. If you are using an IP address of 0.0.0.0, then the last option in "Server configuration" will be "Change DHCP device name". The "Change DHCP device name" option will allow you to change the DHCP name to an alpha numeric name.

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

3) Numeric DHCP name. You are able to change the DHCP name by specifying the last octet of the IP address. When you use this method, the DHCP name will be 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 will be LTX12. This method will only work with 2 digit numbers (0-99).

3.6 Channel 1 Configuration (Serial Port Parameters)

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

```
Baudrate (9600)
I/F Mode (4C)
Flow (00)
Port No (10001)
ConnectMode (C0)
Remote IP Address : (000).(000).(000).(000)
Remote Port (00000)
DisConnMode (00)
FlushMode   (00)
DisConnTime (00:00) :
SendChar 1  (00)
SendChar 2  (00)
```

3.6.1 Baudrate

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

3.6.2 I/F (Interface) Mode

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

Note: See Table 35 - Binary to Hexadecimal Conversion Table.

Table 6 - Interface Mode Options

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

(1) The CoBox-FL requires you to choose the correct setting in the IF mode, and to also set the front-panel switch for selection of RS-232/RS-485.

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

Table 7 - Common Interface Mode Settings

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

(1) The CoBox-FL requires you to choose the correct setting in the IF mode.

3.6.3 Flow

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

Table 8 - 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

3.6.4 Port Number

The setting represents the source port number in TCP connections, and is the number used to identify the channel for remote initiating connections. Default setting for Port 1 is 10001. Range: 0-65535 except for the following reserved port numbers:

Port Numbers	Reserved for
1 – 1024	Reserved (well known ports)
9999	Telnet setup
14000-14009	Reserved
30718	Reserved (77FEh)
10000-10999	Recommended ports, should be used for DeviceComm Manager (COM1-COM256) or direct socket connections

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. Port 0 is used when you want the outgoing source port to change with each connection.

3.6.5 Connect Mode

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

Note: See Table 35 - Binary to Hexadecimal Conversion Table.

Table 9 - Connect Mode Options

Connect Mode Option	7	6	5	4	3	2	1	0
Incoming Connection								
Never accept incoming	0	0	0					
Accept incoming with DTR	0	1	0					
Accept unconditional	1	1	0					
Response								
Nothing (quiet)				0				
Character response (C=connect, D=disconnect, N=unreachable)				1				
Startup								
No active startup					0	0	0	0
With any character					0	0	0	1
With active DTR (1)					0	0	1	0
With CR (0x0D) only					0	0	1	1
Manual connection					0	1	0	0
Autostart					0	1	0	1
Datagram Type								
Directed UDP					1	1	0	0
Modem Mode								
Full Verbose				1	0	1	1	0
Without Echo				0	0	1	1	0
1-character Response				1	0	1	1	1

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

Table 10 - Manual Connection Address Example

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

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

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

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

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

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

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

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

To disconnect a connection using Modem Mode commands:

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

Table 11 - 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: These AT commands are only recognized as single commands like ATE0 or ATV1; compound commands such as ATE0V1 are not recognized. All other AT commands with Modem Mode set to full verbose acknowledge with an OK, but no action is taken.

3.6.6 Remote IP Address

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

3.6.7 Remote Port

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

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

3.6.8 DisConnMode

Note: See Table 35 - Binary to Hexadecimal Conversion Table.

Table 12 - 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 CoBox will send the "Terminal Type" upon an outgoing connection.
2. A password is required for a connection to the serial port from the network.
3. The TCP connection will close even if the remote site does not acknowledge the disconnection.
4. When there is a network connection to or from the serial port, the state LED will turn off instead of blink.
5. When Ctrl D or Hex 04 are detected, the connection is dropped. Both Telnet mode and Disconnect with EOT must be enabled for Disconnect with EOT to function properly. Ctrl D will only be detected going from the serial port to the network.
6. When DTR on the CoBox/UDS product transitions from a high state to a low state, then the network connection to or from the serial port will drop.

3.6.9 Flush Mode (Buffer Flushing)

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

Note: See Table 35 - Binary to Hexadecimal Conversion Table.

Table 13 - 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 UDS to the network				1				
Clear with a connection initiated from the network to the UDS			1					
Clear when the network connection to or from the UDS is disconnected		1						
Output Buffer (Network to Serial)								
Clear with a connection that is initiated from the UDS to the network								1
Clear with a connection initiated from the network to the UDS							1	
Clear when the network connection to or from the UDS is disconnected						1		
Alternate Packing Algorithm (Pack Control)								
Enable	1							

3.6.10 Pack Control

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

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

Note: See Table 35 - Binary to Hexadecimal Conversion Table.

Table 14 - Pack Control Options

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

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

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

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

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

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

3.6.11 DisConnTime (Inactivity Timeout)

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

3.6.12 Send Characters

You can enter up to two characters in hexadecimal representation in the parameters "sendchar." If a character received on the serial line matches one of these characters, it is sent immediately, along with any awaiting characters, to the TCP connection. This minimizes the response time for specific protocol characters on the serial line (for example, ETX, EOT, etc.). Setting the first sendchar to **00** disables the recognition of the characters. Alternatively, the two characters can be interpreted as a sequence (see *Pack Control* on page 3-22).

3.6.13 Telnet Terminal Type

This parameter appears only if the terminal type option is enabled in Disconnect Mode (see *DisConnMode* on page 3-20 above). If this option is enabled, you can use the terminal name for the Telnet terminal type. Enter only one name.

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

3.6.14 Channel (Port) Password

This parameter appears only if the channel (port) password option is enabled in Disconnect Mode (see *DisConnMode* on page 3-20). If set, you can set a password on the serial port.

3.7 Expert Settings

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

Note: The Expert Settings option does not appear with CoBox-FL-IAP.

```
These parameters should only be changed if you are an expert
and definitely know the consequences the changes might have.

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

3.7.1 TCP Keepalive time in s

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

3.8 Security Settings

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

```
Disable SNMP (N)                  (Not with IAP)
SNMP Community Name (public):     (Not with IAP)
Disable Telnet Setup (N)
Disable TFTP Firmware Update (N)
Disable Port 77FEh (N)
Disable Web Server (N)
Enable Enhanced Password (N)
```

3.8.1 Disable SNMP

Note: This option does not appear with CoBox-FL-IAP.

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

3.8.2 SNMP Community Name

Note: This option does not appear with CoBox-FL-IAP.

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

3.8.3 Disable Telnet Setup

This setting defaults to the N (No) option. The Y (Yes) option disables access to this Configuration Menu by Telnet (port 9999). It only allows access via the Web pages and the serial port of the unit.

3.8.4 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, firmware upgrades can be performed only by using a *.hex file over the serial port of the unit.

3.8.5 Disable Port 77FE (Hex)

Port 77FE is a setting that allows DeviceInstaller, Web Pages, and custom programs to configure the unit remotely. You may wish to disable this capability for security purposes. For more information about remote configuration, see the Lantronix Embedded Integration Kit user guide on the Lantronix Web site www.lantronix.com.

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 pages.

Note: The Yes option disables many of the GUI tools for configuring the Device Server, including the embedded Web Page Configuration tool.

3.8.6 Disable Web Server

This setting defaults to the N (option). The Y (Yes) option disables the use of the Web Page Configuration tool that is built into the unit.

3.8.7 Enable Enhanced Password

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

3.9 Factory Defaults

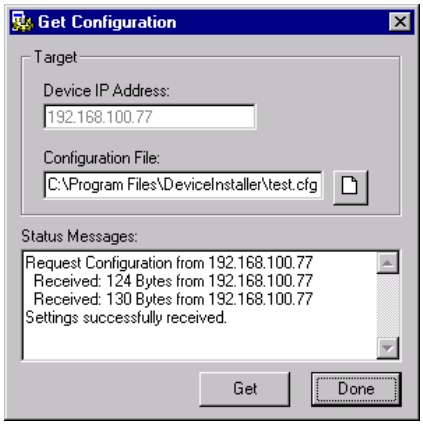
Select **7** to reset the unit's Channel 1 and Enhanced Security to the factory default settings. The server configurations (IP address information) remain unchanged.

3.10 Exit Configuration Mode

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

3.11 Get Configuration

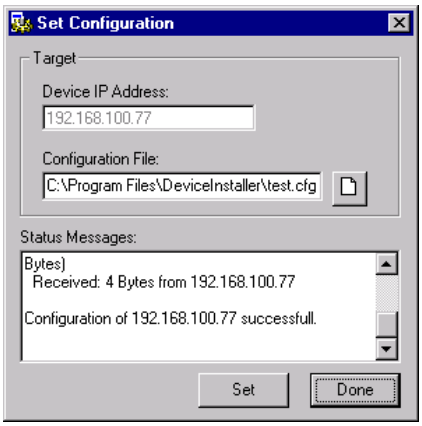
The device configuration information is stored in flash memory and can be read and saved in a configuration file (filename.cfg). To get the configuration information, click the Get Configuration icon button on the Device Management window. The following dialog appears.



The Device IP Address is shown in the first field. This is the device selected in the DeviceInstaller main window. In the Configuration File field, click the Open File button to select a filename for the configuration file. Click the Get button and the file information is read from the device and saved in the selected file.

3.12 Set Configuration

Device configuration information can be saved in a file and later used to set the configuration of one or several devices. To set the configuration of a device from a saved file, click the Set Configuration button on the Device Management window. The following dialog appears.



The Device IP Address is shown in the first field. This is the device selected in the DeviceInstaller main window. In the Configuration File field, click the Open File button to select a configuration file. Click the Set button and the file information is read and stored in the device.

4. Updating Protocol (Firmware)

4.1 Protocol Firmware

You can update the unit's internal operational code to a newer revision, or change the code to operate with a specific vendor.

The CoBox-FL-IAP was designed to allow loading of vendor specific protocol firmware. This firmware takes the place of the IAP Standard Tunnel Protocol. Vendor specific protocols and the software tools needed to load them can be found on the software CD.

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

Once you load a vendor specific protocol, you must reference the user manual associated with that protocol, since many of the setup and configuration dialogs will be changed. Some features, such as web pages, may not be available with certain vendor protocols.

Note: If you change the protocol to a vendor specific protocol, you MUST reference the associated protocol manual for setup and configuration information. The menu options shown in this manual are for Standard Tunnel Protocol.

4.2 Reloading Protocol Firmware

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

The firmware files are located on the software CD in the **firmware** folder. Here is a list of *typical* names for those files. Check the Lantronix web site for the latest versions and release notes.

Table 15 - Protocol Firmware

Folder Name	ROM File	COB
AD - DF1 MultiMaster	DF1 Multi-master ad0100.rom (IAP only)	NA
AM - Modbus Bridge	AM0144.rom (IAP only)	NA
AQ - Standard	Standard Tunnel aq0100.rom (IAP only)	(Standard Tunnel_aq0100wb6.cob) (or cbxw300.cob)
CoBox-FL	ltx45.rom	cbxw300.cob

4.2.1 Via DeviceInstaller

After downloading the firmware to your computer, or locating the file on your software CD, you can use DeviceInstaller to install it.

1. Download the updated firmware files from www.lantronix.com or ftp.lantronix.com and store them in a subfolder on your computer.
2. Click the **Start** button on the Task Bar and select **Programs\DeviceInstaller\Device Installer**. The Device Installer window displays.

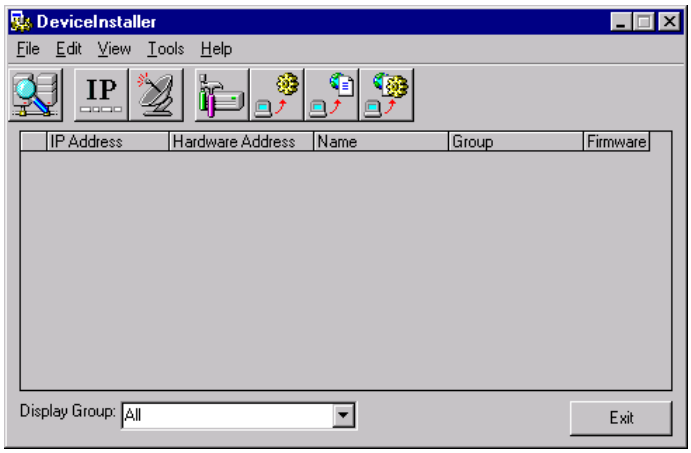


Figure 14 - Device Installer

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

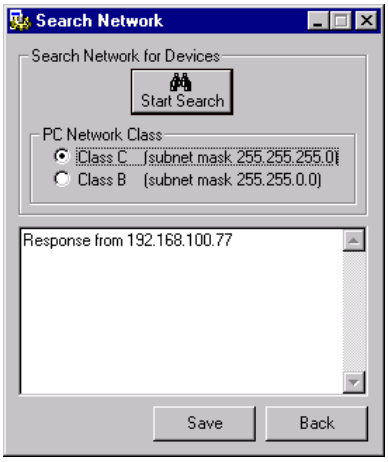


Figure 15 - Search Network Window

4. Click the **Start Search** button. A list of all active units on the local network displays.
5. Click the **Save** button. A confirmation message displays.
6. Click O**K**.
7. Click the **Back** button to return to the Device Installer window. The Device Installer window now lists all of the devices in the group, including the unit you are updating.

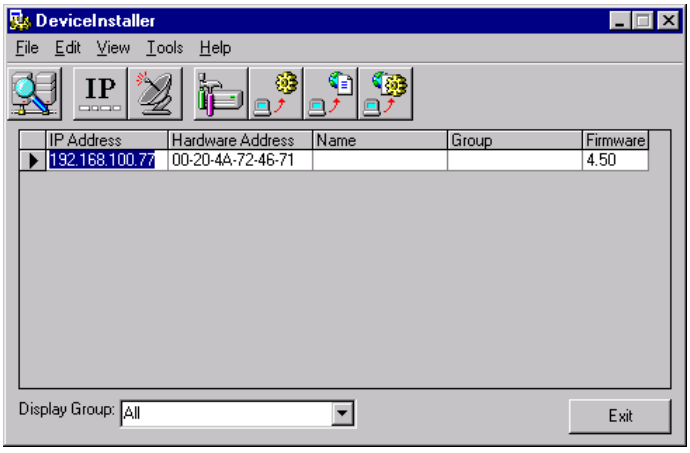


Figure 16 - Devices in a Group

8. Select the desired unit and click the **Upgrade Firmware file (.ROM)** icon . The Upgrade Firmware window displays.

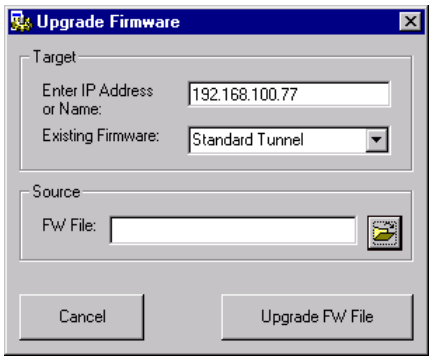


Figure 17 - Upgrade Firmware

9. In the **Existing Firmware** list box, select the firmware type that is currently in the unit. This selection must match the Firmware file type currently installed or an error message will be displayed.
10. In the **Source FW File** field, locate the firmware file from the software CD or the file you downloaded from the Lantronix web site.
11. Click the **Update FW File** button. Upgrade status process messages display in the lower part of the window. When the process is complete, the "File upgrade successful" message displays.
12. Click **OK**.

*Note: You can update the unit's Web pages by clicking the **Upgrade Web files (.COB)** icon. Though it would be rare to need to update both the firmware and Web pages at the same time, you can do so by clicking the **Update the firmware files and Webpages in one step** icon.*

4.2.2 Via 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. Make sure the **Put** and **Binary** options at the top of the window are selected.
3. Enter the full path of the firmware file in the **Source File** field.

4. In the **Destination File** field, enter the **current** internal operational code or **WEB5** for the internal Web interface. (For CoBox-FL-IAP, AQ = Standard Tunnel, AM = Modbus, AD = DF1. For CoBox-FL, 3Q = Standard Tunnel)
5. In the **Remote Host** field, enter the IP address of the unit being upgraded.
6. Click the **Put** button to transfer the file to the unit.

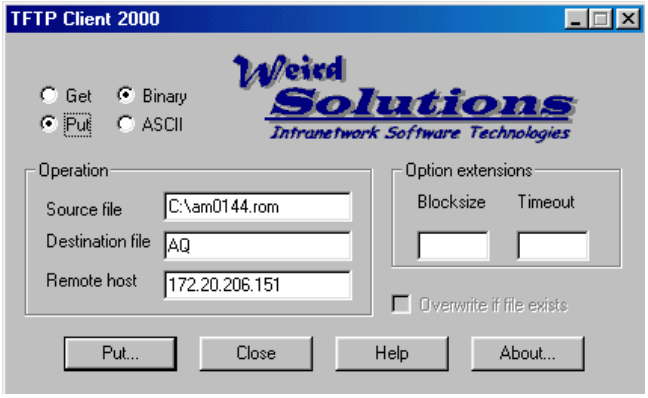


Figure 18 - TFTP Dialog Box

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

4.2.3 Via Another Unit

To distribute firmware to another unit over the network:

1. Enter the host unit's Monitor Mode (see *Monitor Mode* on page 7-1).
2. Send the firmware to the receiving unit using the **SF** command, where x.x.x.x is the receiving unit's IP address.

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

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

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

4.2.4 Via the Serial Port

The following procedure is for using the HyperTerminal software application. In some cases, the HEX format file is available on the software CD and on the Web site.

Before you can load firmware through the serial port you need to convert the ROM code to HEX format. There is a DOS application, R2H.EXE that can be used to convert the ROM file to HEX format. The R2H.EXE application is available at ftp://ftp.lantronix.com/pub.

Put R2H.EXE and the *.ROM file into the same directory on a PC then open a DOS Window to that directory and type:

C:\ R2H *filename*

This will create a filename.hex file that you can load via the serial port.

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

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

1. Enter Monitor Mode via the serial port. (see *Monitor Mode* on page 7-1).
2. Download the firmware to the unit using the **DL** command.
3. Select **Send Text File** and select the *.HEX file to be downloaded. The downloaded file must be the **.HEX** (ASCII) version.
4. After the final record is received, the unit checks the integrity of the firmware image before programming the new firmware in the flash ROM. The following message displays when the firmware upgrade is complete.

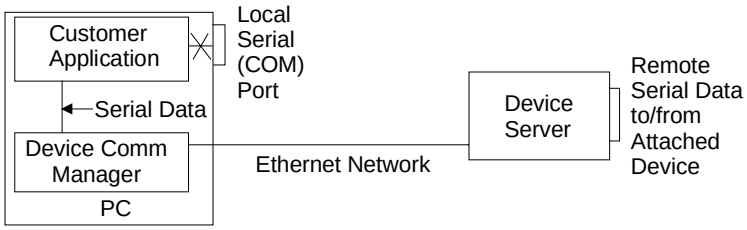
```
*** NodeSet 2.0 ***
0>DL
02049 lines loaded.
```

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

5. DeviceComm Manager

Lantronix DeviceComm Manager is a Windows based COM port redirector software utility. Its function is to redirect customer application data destined for a local serial (COM) port to the PC's network port. Rather than going out the local serial port, the data is transmitted across the Ethernet network port using the TCP/IP protocol.

A Device Server attached to the network receives the data and presents it on its serial port. Conversely, data into the serial port of the Device Server is sent back over the network to the DeviceComm Manager. The DeviceComm Manager then presents the data to the customer application as if it were from a local serial COM port.



This powerful 32-bit Windows utility allows any commercially available or application-specific software to communicate with networked devices as if they were directly attached to the PC's COM ports. To the user, this means that when they network-enable a serial device with a Lantronix Device Server, they can retain their existing PC-based applications software without having to undertake the additional time and expense of developing new software.

Using simple on-screen menus, users can map up to 255 COM ports directly to IP addresses assigned to Lantronix Device Servers. Once COM ports are mapped, any networked PC with DeviceComm Manager software installed can access devices on the network via Lantronix' Device Servers. Both the software application and the serial device operate normally as if they were still directly connected - Lantronix Device Server and the DeviceComm Manager utility do all the work in between to keep data flowing smoothly.

The DeviceComm Manager utility consists of a Control Panel applet, a device driver, and a Windows service.

- Eliminates the need for the users to develop or modify their existing application software
- No understanding of how to develop networking software is required
- Everything is totally transparent to the serial device, the application software, and the user
- Redirects up to 255 COM ports simultaneously over TCP/IP protocol
- Provides raw mode data only, which means it will not change or modify the data being sent
- Supports Windows 2000, Windows NT4.0, and Windows XP
- Easy to install and even easier to configure

5.1 Installing DeviceComm Manager

The DeviceComm Manager software is included on the product CD or it can be downloaded from the Lantronix web site.

5.1.1 Install DeviceComm Manager

1. Insert the product CD into your CD-ROM drive. The CD will automatically start and display the main window.

   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, devicecomm.exe (e.g., D:\devicecomm.exe).

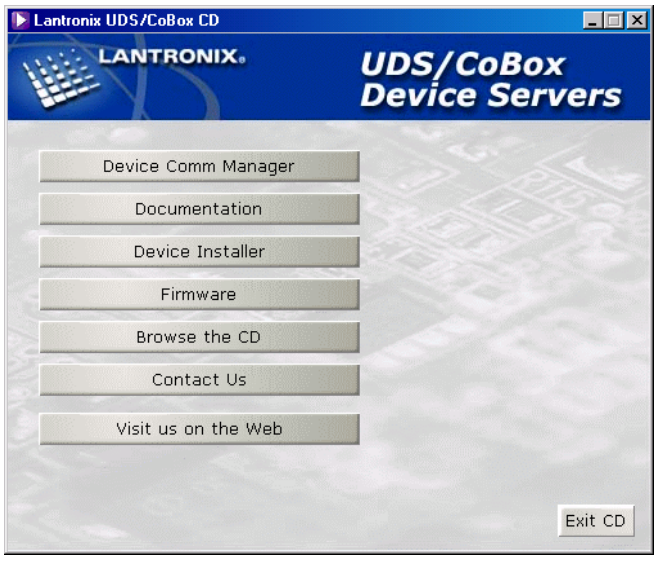


Figure 19 – UDS/CoBox Main Window

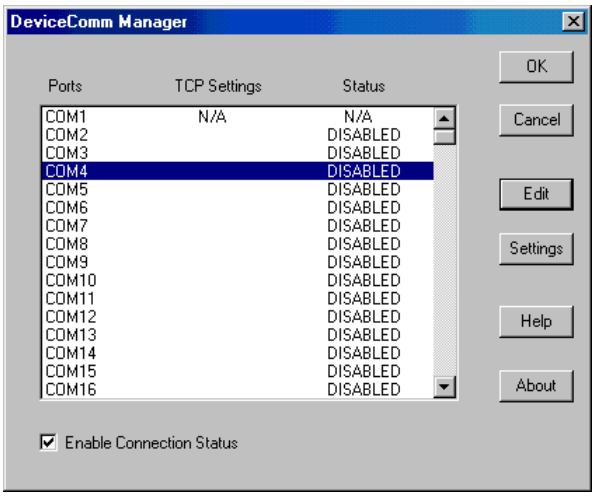
2. Click the **DeviceComm Manager** button. The installation wizard window displays.

Respond to the installation wizard prompts.

Note: DeviceComm Manager is installed in the Control Panel.

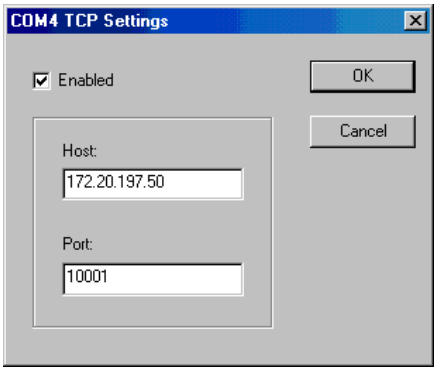
5.1.2 Setup

1. Open Control Panel.
2. Double click on the "DeviceComm Manager" Icon  .



Status	Meaning
DISABLED	Unused port on your system
N/A	Port being used by other hardware / software on your system
IDLE	An IP address and port number have been associated with the COM port
CONNECTED	An active TCP/IP connection exists between the COM port and the device server

3. Select one of the **DISABLED** ports by clicking on it, and then press the **Edit** button.



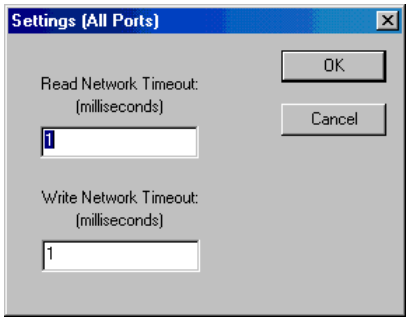
4. Select the **Enabled** check box.
5. Type in the IP address of the target device server in the "Host:" section.

6. Enter the Port number of the target device server in the “Port:” section. Click **OK** when done.

   ****Please Note:****
   Because this is a raw mode redirector:
   a. On UDS and CoBox products, you cannot use ports 14000 through 14009.
   b. On MSS, ETS, LRS, and SCS products DO use the 3001, 3002, 3003, etc. ports.

Note: You will be required to reboot your system when enabling COM ports. You may want to set them all up at one time and then reboot.

7. Click the **Settings** button for advanced configuration. Some serial applications do not work well when redirected because they are not expecting the latency (delay) that an Ethernet network may cause. Increasing the “Read Network Timeout” and the “Write Network Timeout” values may help the situation. Network latency varies depending on a number of factors. You can get a rough idea of the delay at a given time by “pinging” the device server from the PC and looking at the “time” column. You may also find the PC command “tracert” helpful. See your Windows OS documentation for more details on these commands. Both “ping” and “tracert” are DOS prompt commands.



8. Click Ok to close the Settings dialog box.
9. Select the "Enable Connection Status” checkbox at the bottom of the **DeviceComm Manager** screen if you wish to be notified via screen pop-up when the connection to the remote port is established. If your application is very time sensitive regarding the initial connection, or you do not wish to have a screen pop-up, leave this box unchecked.
10. Click OK to complete the setup.

No other setup is required. In the above example, all data sent to COM4 will be sent across the network to the device server at “172.20.197.50”, port “10001”.

6. Troubleshooting

6.1 Technical Support

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.

6.1.1 Technical Support

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

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

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

Technical Support Europe, Middle East, and Africa
+49 (0) 7720 3016 20/57

eu_techsupp@lantronix.com

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

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

When troubleshooting the following problems, make sure that the CoBox-FL is powered up and the Link (L) LED is lit solid green. If the Link LED is not lit, then the physical network connection is bad. Confirm that you are using a good network connection.

Table 16 - 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 attempted to assign an IP address to the UDS/CoBox via the ARP method, the "Press Enter to go into Setup Mode" error (described below) displayed. Now when you Telnet to the UDS/CoBox, the connection fails.	When you Telnet into port 1 on the UDS/CoBox, you are only assigning a temporary IP address. When you Telnet into port 9999 and do not press Enter quickly, the UDS/CoBox will reboot, causing it to lose the IP address.	Telnet back into Port 1. Wait for it to fail, then Telnet to port 9999 again. Make sure you press Enter quickly.
When you Telnet to port 9999, the message "Press Enter to go into Setup Mode" displays. However, nothing happens when you press Enter, or your connection is closed.	You did not press Enter quickly enough. You only have 5 seconds to press Enter before the connection is closed.	Telnet to port 9999 again, but press Enter as soon as you see the message "Press Enter to go into Setup Mode."
When you Telnet to port 1 to assign an IP address to the UDS/CoBox, the Telnet window does not respond for a long time.	You may have entered the Ethernet address incorrectly with the ARP command.	Confirm that the Ethernet address that you entered with the ARP command is correct. The Ethernet address may only include numbers 0-9 and letters A-F. In Windows and usually in Unix, the segments of the Ethernet address are separated by dashes. In some forms of Unix, the Ethernet address is segmented with colons.

Problem/Message	Reason	Solution
	The IP address you are trying to assign is not on your logical subnet.	Confirm that your PC has an IP address and that it is in the same logical subnet that you are trying to assign to the UDS/CoBox.
	The UDS/CoBox 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 UDS/CoBox is not properly plugged into the network.
When you try to assign an IP with Device Installer, you get the following message: "No response from device! Verify the IP, Hardware address and Network Class. Please try again."	The cause is most likely one of the following: The Hardware address you specified is incorrect. The IP address you are trying to assign is not a valid IP for your logical subnet. You did not choose the correct subnet mask.	Double-check the parameters that you specified. Tip: You cannot assign an IP address to a UDS/CoBox through a router.
No LEDs are lit.	The unit or its power supply is damaged.	Change power supplies.
The UDS/CoBox will not power up properly, and the LEDs are flashing.	Various	Consult the LEDs section in the Introduction chapter or the Quick Start for the LED flashing sequence patterns. Call Lantronix Technical Support if the blinking pattern indicates a critical error.
The UDS/CoBox 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 UDS/CoBox must match. The default serial settings for the UDS/CoBox are RS232, 9600 Baud, 8 Character Bits, No Parity, 1 Stop Bit, No Flow Control.
When you try to enter the setup mode on the UDS/CoBox via the serial port, you get no response.	The issue will most likely be something covered in the previous problem, or possibly you have Caps Lock on.	Double-check everything in the problem above. Confirm that Caps Lock is not on.
You can ping the UDS/CoBox, but not Telnet to the UDS/CoBox on port 9999.	There may be an IP address conflict on your network You are not Telneting to port 9999. The Telnet configuration port (9999) is disabled within the UDS/CoBox security settings.	Turn the UDS/CoBox 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 UDS/CoBox) PING X.X.X.X (X.X.X.X is the IP of the UDS/CoBox). If you get a response, then there is a duplicate IP address on the network (the LEDs on the UDS/CoBox should flash a

Problem/Message	Reason	Solution
		sequence that tells you this). If you do not get a response, use the serial port to verify that Telnet is not disabled.
With Device Installer you get the “Wrong Password” error when you try to upgrade the firmware.	You have chosen the incorrect setting for the **Existing Firmware** field.	Try upgrading the firmware again, but make sure to use the correct setting in the field of **Existing Firmware** field.
When connecting to the Web-Manager within the UDS/CoBox, the message “No Connection With CoBox” displays.	Your computer is not able to connect to port 30718 (77FEh) on the UDS/CoBox.	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 UDS/CoBox.

7. Monitor Mode

7.1 Monitor Mode

Monitor Mode is a command-line interface used for diagnostic purposes (see *Table 17 - Monitor Mode Commands*). There are two ways to enter Monitor Mode: locally via the serial port or remotely via the network.

7.1.1 Entering Monitor Mode Via the Serial Port

To enter Monitor Mode locally:

1. Follow the same principles used in setting the serial configuration parameters (see *Configuring via the Setup Mode Window* on page 3-10.
2. Instead of typing three "x" keys, however, type zzz (or xxl) to enter Monitor Mode with network connections.

Type yyy (or yyy) to enter Monitor Mode without network connections.

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

7.1.2 Entering Monitor Mode Via the Network Port

To enter Monitor Mode using a Telnet connection:

4. First establish a Telnet session to the configuration port (9999). The following message appears:

```
Serial Number 1400280  MAC address 00:20:4A:14:01:18
Software Version 4.3 (xxxxxx)
Press Enter to go into Setup Mode
```

5. Type M (upper case).

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

7.1.3 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 the IP address is given, the command is applied to another Device Server with that IP address. If no IP address is given, the command is executed locally.

Note: All commands must be given in capital letters.

Table 17 - Monitor Mode Commands

Command	Command Name	Function
DL	Download	Download firmware to the Device Server via the serial port in hex format
SF x.x.x.x	Send Firmware	Send firmware to Device Server with IP address x.x.x.x
VS x.x.x.x	Version	Query software header record (16 bytes) of Device Server with IP address x.x.x.x
GC x.x.x.x	Get Configuration	Get configuration of Device Server with IP address x.x.x.x as hex records (120 bytes)
SC x.x.x.x	Send Configuration	Set configuration of Device Server with IP address x.x.x.x from hex records
PI x.x.x.x	Ping	Ping Device Server with IP address x.x.x.x to check device status
AT	ARP Table	Show the Device Server's ARP table entries
TT	TCP Connection Table	Shows all incoming and outgoing TCP connections
NC	Network Connection	Shows the Device Server's IP configuration
RS	Reset	Resets the Device Server's power
SI xxx.xxx.xxx.xxx: yyy.yyy.yyy.yyy	Send/Set IP Address	Remotely assign an IP address to a Device Server, where xxx.xxx.xxx.xxx is the IP address, and yyyy.yyy.yyyy.yyy is the two-part identification number at the bottom of the label, converted to decimal, and written twice.
QU	Quit	Exit 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 (see *The Intel Hex Format* on page 8-5).

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

Table 18 -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. Network Configuration using UDP

8.1 UDP Datagrams

The Device Server can also be configured or queried over the network using UDP datagrams. The Device Server has a UDP listener set for port 30718 (77FE Hex). Responses from the Device Server are returned to the source port of the UDP packet.

The first three bytes of the UDP data block should be set to zero. The fourth byte selects the function as described in the following table:

Table 19 - UDP Configuration

Byte	Command	Parameters	Notes
03	Node Reset	2 bytes, software type	These 2 bytes are used to prevent accidental reset of the Device Server. (Value for standard CoBox firmware: 33 51 [Hex], 3Q)
F6	Query for Firmware Version	None	The Device Server responds with the F7 block below.
F7	Firmware Information	First 16 bytes of the firmware image, and 4 bytes device information and serial number.	The first 16 bytes of the firmware image contain the software type (offset 4,5) and checksum (offset 14,15). The last two bytes of the device information contain the serial number.
F8	Query for Setup Record	None	The Device Server responds with the F9 block below.
F9	Configuration Readback	120 byte setup record (see Setup Records on page E-7)	n/a
FA	Set Configuration	120 byte setup record (see Setup Records on page E-7)	The IP address (byte 0-3) will not be overridden using FA. See FD for this functionality.
FB	Configuration Change Acknowledge	None	This block is sent back to the host requesting a configuration change (FB). After sending out this block, the Device Server resets and uses the new configuration sent with the FA command.
FC	Set IP Address	First 8 bytes must be set to the string	This block can be sent as a broadcast, because the serial number is unique. It

Byte	Command	Parameters	Notes
		IP-SETUP (Hex 49 50 2D 53 45 54 55 50). Next 2 bytes have to be set to 00. Next 2 bytes must contain the serial number. Next 4 bytes have to be the new IP address.	provides one method to set the IP address of the Device Server if is on the local network and the serial number is known. Remember, broadcasts are only 'heard' on the subnet on which they are generated. No reply is sent by the Device Server, which restarts using the new IP address after the block is received. Example (all in Hex): 49 50 2D 63 45 54 55 50 00 00 2A 12 81 00 01 02 IP address of the node with serial number 42-18 set to 129.0.1.2
FD	Set Configuration and IP Address	Same as FA, but changes IP address as well (bytes 0-3).	n/a

8.2 Configuring Multiple Devices

When configuring a number of Device Servers identically, it is useful to create a template setup record. The setup record can then be sent to the "target" Device Servers from a "master" Device Server via "cut and paste" or UDP (see *Network Configuration using UDP* on page 8-1).

Device Servers use a 120-byte setup record in Intel Hex format. This format facilitates the transfer of binary data using ASCII characters. See *Setup Records* on page 8-7 and *The Intel Hex Format* on page 8-5 for information about setup records and converting them to Intel Hex format.

```
:20000010AC10C81D00001000000000000AC10010B4C020000112700000000000C000
000011
:2000201000000000000000000000000000000000000000000000000000000000000
0000B0
:200040104C020000122700000000000C000000000000000000000000000000000000
000049
:18006010000000000000000000000000000000000000000000000000000078
:00000001FF
```

Figure 20 - Sample Setup Record in Intel Hex Format

8.2.1 Acquiring a Valid Setup Record

There are a number of ways to acquire a valid setup record:

- Copy the setup record of a properly configured Device Server via Monitor Mode (easiest method).
- Request the setup record of a properly configured Device Server via another Device Server on the network.
- Build the setup record in software.
- From a host PC, request the setup record of a properly configured Device Server via UDP.

To copy the setup record of a properly configured Device Server:

1. Configure a "master" Device Server with the desired parameters.
2. Enter Monitor Mode on the master Device Server (see *Monitor Mode* on page 7-1).
3. At the prompt, enter GC followed by a carriage return. The Device Server will respond with its setup record in Intel Hex format.
4. Copy the setup record into a text file and save it for future use.

To request the setup record of a properly configured Device Server via another Device Server on the network:

5. Make sure that both units are plugged onto the network properly.
6. Enter Monitor Mode (with network support enabled) on the unit that is not properly configured. (see *Monitor Mode* on page 7-1)
7. Issue the command GC x.x.x.x followed by a carriage return, where x.x.x.x is the IP address of the properly configured device. The properly configured device will respond by sending its setup record to the unit you are currently on. This configuration will be displayed in Intel HEX format.
8. Copy that HEX string, and then issue the command SC. Now paste the copied string.

The unit will not reboot on its own. You must reboot the unit before the settings take effect.

To build the setup record in software:

1. Create a 120-byte setup record.
2. Convert it to an Intel Hex record (see *The Intel Hex Format* on page 8-5).
3. Copy the setup record into a text file and save it for future use.

To request the setup record of a properly configured Device Server via UDP:

1. Configure a Device Server with the desired parameters and place it on the network.
2. From a host PC, send the F8 datagram to the Device Server (see *Network Configuration using UDP* on page 8-1). The Device Server responds with the F9 datagram, which includes its setup record.
3. Send a previously saved setup record from a host PC via UDP.

8.2.2 Sending a Setup Record

There are also a number of ways to send a setup record to a Device Server:

- Send a previously saved setup record via Monitor Mode (easiest method).
- Send the setup record of a properly configured Device Server to another Device Server on the network.
- Send a previously saved setup record from a host PC via UDP.

To send a setup record via Monitor Mode:

1. Configure a "master" Device Server with the desired parameters and place it on the network.
2. Place another Device Server (the "target") on the network.
3. Enter Monitor Mode (with network support enabled) on the master Device Server (see *Monitor Mode* on page 7-1)
4. At the prompt, enter SC, the IP address of the target, and a carriage return.
5. Send the setup record to the target Device Server.

Note: For example, using Hyperterminal, copy the setup record and select "Paste to Host" to send it to the Device Server. The Device Server reboots with the new configuration.

To send a previously saved setup record to a Device Server via UDP, from a host PC, send the **FA** (or **FD**) datagram to the "target" Device Server (see *Network Configuration using UDP* on page 8-1).

Note: The Device Server responds with the FB datagram. Refer to the table.

8.2.3 The Intel Hex Format

With this format, 8-bit binary data can be sent and received as ASCII text. The transmission is blocked in records, and every record has its own checksum.

The record begins with a colon (:) and consists of a block length (2-character Hex), a 16-bit address (4-character Hex), and a block type (2-character Hex). It is built by adding all binary 8-bit values and taking the complement, so adding all byte values (including length, address, and type) should yield zero.

Example:

```
00000001FF
```

End record, type 01, length 00, address 00 00, checksum FF.

```
01002000805F
```

Data record consisting of one byte (value 80 Hex) for address 0020 (32 decimal).

For communication with the node, the following block types are defined:

Table 20 - Block Types

Option	Hex
Data block program memory (firmware)	00
End record	01
Data block configuration memory	10

To get and set the node configuration, 120 bytes should be exchanged at once in 32-Byte records. The IP address in the record (bytes 0 to 3) will be ignored (unless the UDP FD command is being used).

8.2.4 Calculating the Checksum

As mentioned in *Table 20 - Block Types* above, the last two characters of an Intel Hex setup record represent a checksum of the data in the line. Since the checksum is a two-digit hexadecimal value, it can represent a value from 0 to 255.

The checksum is calculated by summing the value of the data on the line and taking the two's complement of the sum.

Note: Do not include the leading colon or the checksum byte in the sum.

Example:

```
0300300002337A1E
```

Record length: 03 (3 bytes of data)
Address: 0030 (the 3 bytes will be stored at 0030, 0031, and 0032)
Record Type: 00 (normal data)
Data: 02, 33, 7A
Checksum: 1E

03 + 00 + 30 + 00+ 02 + 33 + 7A = E2

The two's complement of E2 is 1E. See *Calculating the Two's Complement* below.

8.2.5 Calculating the Two's Complement

The two's complement of a number is the value that must be added to the number to reach a Hexadecimal value of 100 (256 in decimal). In the example above, E2 + 1E = 100.

You can also calculate the two's complement by subtracting the sum from 100. Using the example above again, 100 - E2 = 1E. It may help to use a scientific calculator.

8.3 Setup Records

A setup record consists of 120 bytes. They are transmitted at once from and to the node. Unused bytes should be initialized as 00. *Table 21 - Setup Record Construction* defines the structure of a setup record:

Table 21 - Setup Record Construction

Byte(s)	Function
00-03	IP address of the unit (x.x.x.x)
04	Reserved (0)
05	Flag BYTE Bit 7: Reserved (0) Bit 6: Set 1 for AUI, 0 for 10BASE-T (CoBox-Micro only) Bits 5-0: Reserved (0)
06	Number of host bits for subnetting; if 0, matching standard netmask for Class A, B, C is used.
07	Reserved (0)
08-11	Telnet configuration password (0 if not used)
12-15	Gateway IP address (0,0,0,0 if not used)
16-63	48-byte Channel 1 parameters; parameter setup Channel 1 (see Table E-4: Channel Parameters)
64-111	48-byte Channel 2 parameters; parameter setup Channel 2 (see Table E-4: Channel Parameters))
112-119	Reserved (0)

8.3.1 Channel Parameters

Use the following table to select setup record parameters for Channels 1:

Table 22 - Channel Parameters

Byte(s) (Channel 1)	Function
16	Interface Mode (see *Table 23 - Interface Mode Options*)
17	Line Speed Bits 7-5: Reserved Bits 4-0: Baud Rate (see *Table 25 - Baud Rate Settings*)
18	Flow Control (see *Table 26 - Flow Control Options*)
19	Reserved
20-21	Own TCP port low-byte, high-byte (Intel)
22-23	Remote TCP port low byte, high-byte (Intel)
24-27	Remote IP address (low/high low/high)
28	Connect Mode (see *Table 27 - Connect Mode Options*)
29	Disconnect Mode (see *Table 28 - Disconnect Mode Options*)
30	Disconnect w/ inactivity time-out, minutes (00 if unused)
31	Disconnect w/ inactivity time-out, seconds (00 if unused)
32-33	Characters to trigger send immediately (sendchar)
34	Flush mode (see *Table 29 - Flush Mode Options*)
35	Pack Control (see *Table 30 - Pack Control Options*)
36-47	Reserved (0)
48-63	a) Terminal name for Telnet terminal type option (15 characters max), 0-terminated. If set and Bit 6 in Disconnect Mode is set, Telnet connection will be assumed. b) Password for Passworded Socket Connection (Bit 4 in Disconnect Mode Set).

8.3.2 Interface Mode

The Interface (I/F) Mode is a bit-coded byte entered in hexadecimal notation. Use the following table to select Interface Mode settings:

Table 23 - Interface Mode Options

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

(1) The CoBox-FL requires you to choose the correct setting in the IF mode.

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

Table 24 - Common Interface Mode Settings

Option	Binary	Hex
RS-232C, 8-bit, No Parity, 1 stop bit (1)	0100 1100	4C
RS-232C, 7-bit, Even Parity, 1 stop bit (1)	0111 1000	78
RS-485 2-Wire, 8-bit, No Parity, 1 stop bit (1)	0100 1111	4F
RS-422, 8-bit, Odd Parity, 2 stop bits (1)	1101 1101	DD

(1) The CoBox-FL requires you to choose the correct setting in the IF mode.

Note: See Table 35 - Binary to Hexadecimal Conversion Table.

8.3.3 Baud Rate

The Device Server and attached serial device must agree on a speed or baud rate to use for the serial connection. Use the following table to select Baud Rate settings:

Table 25 - Baud Rate Settings

Speed (bps)	Hex
38400	00
19200	01
9600	02
4800	03
2400	04
1200	05
600	06
300	07
115200	08
57600	09

8.3.4 Flow Control

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 26 - Flow Control Options

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

8.3.5 Connect Mode

Connect Mode defines how the Device Server makes a connection, and how it reacts to incoming connections over the network. Use the following table to select Connect Mode options:

Table 27 - Connect Mode Options

Connect Mode Option	7	6	5	4	3	2	1	0
Incoming Connection								
Never accept incoming	0	0	0					
Accept incoming with DTR	0	1	0					
Accept unconditional	1	1	0					
Response								
Nothing (quiet)				0				
Character response (C=conn, D=disconn, N=unreachable)				1				
Startup								
No active startup					0	0	0	0
With any character					0	0	0	1
With active DTR (1)					0	0	1	0
With CR (0x0D) only					0	0	1	1
Manual connection					0	1	0	0
Autostart					0	1	0	1
Datagram Type								
Directed UDP					1	1	0	0
Modem Mode								
Full Verbose				1	0	1	1	0
Without Echo				0	0	1	1	0
1-character Response				1	0	1	1	1

Note: See Table 35 - Binary to Hexadecimal Conversion Table.

8.3.6 Disconnect Mode

In Disconnect Mode, DTR drop either drops the connection or is ignored. Use the following table to select Disconnect Mode Options:

Table 28 - 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 CoBox will send the "Terminal Type" upon an outgoing connection.
2. A password is required for a connection to the serial port from the network.
3. The TCP connection will close even if the remote site does not acknowledge the disconnection.
4. When there is a network connection to or from the serial port, the state LED will turn off instead of blink.
5. When Ctrl D or Hex 04 are detected, the connection is dropped. Both Telnet mode and Disconnect with EOT must be enabled for Disconnect with EOT to function properly. Ctrl D will only be detected going from the serial port to the network.
6. When DTR on the CoBox/UDS product transitions from a high state to a low state, then the network connection to or from the serial port will drop.

Note: See Table 35 - Binary to Hexadecimal Conversion Table.

8.3.7 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. Use the following table to select Flush Mode options:

Table 29 - 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 UDS to the network				1				
Clear with a connection initiated from the network to the UDS			1					
Clear when the network connection to or from the UDS is disconnected		1						
Output Buffer (Network to Serial)								
Clear with a connection that is initiated from the UDS to the network								1
Clear with a connection initiated from the network to the UDS							1	
Clear when the network connection to or from the UDS is disconnected						1		
Alternate Packing Algorithm (Pack Control)								
Enable	1							

Note: See Table 35 - Binary to Hexadecimal Conversion Table.

8.3.8 Pack Control

Alternate packing algorithm settings are enabled in Flush Mode. Use the following table to select Pack Control options:

Table 30 - Pack Control Options

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

8.4 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 Device Server must be assigned a unique IP address to use TCP/IP network functionality.

IP addresses contain three pieces of information: the network, the subnet, and the host.

8.4.1 Network Portion

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

Table 31 - 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 32 - Available IP Addresses

Class	Reserved	Available
A	0.0.0.0 127.0.0.0	1.0.0.0 to 126.0.0.0
B	128.0.0.0 191.255.0.0	128.1.0.0 to 191.254.0.0
C	192.0.0.0 223.255.255.0	192.0.1.0 to 223.255.254.0
D, E	224.0.0.0 to 255.255.255.254 255.255.255.255	None (Check this)

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.

8.4.2 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.

8.4.3 Host Portion

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

8.4.4 Network Address

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

```
192.168.0.0
```

8.4.5 Broadcast Address

A host address with all host bits set to 1 is the broadcast address, meaning for "for every station."

```
192.168.0.255
```

Network and broadcast addresses must not be used 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 IP address differently than 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 Device Server prompts for the number of host bits to be entered and then calculates the netmask, which is displayed in standard decimal-dot notation (for example, 255.255.255.0) when saved parameters are displayed.

Table 33 - 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 34 - 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

8.4.6 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 Device Server on an intranet, you should use one of the reserved sub-networks. Consult your network administrator with questions about IP address assignment.

8.4.7 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

9. Binary to Hex Conversion

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.

Table 35 - 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

9.1 Connect Mode Options

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

Binary to Hex

Table 36 - 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

Accept Incoming Connections	Serial Response Upon Connection	Active Connection Startup	Hostlist	Hex
Unconditionally	Character	Autostart		D5
Unconditionally	Character	UDP		DC
Never	None (quiet)	No active startup	Hostlist	N/A
Never	None (quiet)	Any character	Hostlist	21
Never	None (quiet)	Active DTR	Hostlist	22
Never	None (quiet)	CR (0x0D)	Hostlist	23
Never	None (quiet)	Manual connection	Hostlist	N/A
Never	None (quiet)	Autostart	Hostlist	25
Never	None (quiet)	UDP	Hostlist	
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

Binary to Hex

Accept Incoming Connections	Serial Response Upon Connection	Active Connection Startup	Hostlist	Hex
Unconditionally	Character	Autostart	Hostlist	F5
Unconditionally	Character	UDP	Hostlist	N/A

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

Table 37 - 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

9.2 Disconnect Mode Options

Table 38 - Disconnect Mode Options

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

Binary to Hex

Disconnect with DTR Drop (Note)	Telnet Mode and Terminal Type Setup	Channel (port) Password	Hard Disconnect	State LED Off with Connection	Disconnect with EOT (^D)	Hex
	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

9.3 Flush Mode (Buffer Flushing) Options

Table 39 - 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

Binary to Hex

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

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

Binary to Hex

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

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

Binary to Hex

Serial to Network **Clear input buffer upon:**	**Network to Serial** **Clear output buffer upon:**	**Alternate Packing Algorithm**	**Hex**
Passive connection Disconnect	Active connection Passive connection 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

9.4 Interface Mode Options

Table 40 - Interface Mode Options

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

9.5 Pack Control Options

Table 41 - Pack Control Options

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

Sendcharacter Defined by a:	Trailing Characters	Idle Time Force Transmit:	Send Immediately after Sendcharacter	Hex
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

10. IP Addresses

An IP address is a 32-bit value, divided into four octets of eight bits each. The standard representation is four decimal numbers (in the range of 0..255) divided by dots.

```
192.2.1.123
```

This is called decimal-dot notation.

The IP address is divided in two parts: network and host. To support different needs, three *network classes* have been defined. Depending on the network class, the last one, two or three bytes define the host, while the remaining part defines the network. In the following explanations, ***x*** stands for the host part of the IP address:

10.1 Class A Network

IP address 1.x.x.x to 127.x.x.x

Only 127 different networks of this class exist. These have a very large number of potential connected devices (up to 16,777,216).

Example: 10.0.0.1, (network 10, host 0.0.1)

10.2 Class B Network

IP address 128.0.x.x to 191.255.xxx.xxx

These networks are used for large company networks. Every network can consist of up to 65,534 devices.

Example: 172.1.3.2 (network 172.1, host 3.2)

10.3 Class C Network

IP address 192.0.0.xxx to 223.255.255.xxx

These network addresses are most common and are often used in small companies. These networks can consist of a maximum number of 254 hosts.

Example: 192.7.1.9 (network 192.7.1, host 9)

The remaining addresses 224.x.x.x - 239.x.x.x are defined as ”class D” and are used as multicast addresses.

The addresses 240.x.x.x. - 254.x.x.x are defined as class E and are reserved addresses.

10.4 Network Address

The host address with all host bits set to 0 is used to address the network as a whole (in routing entries, for example).

10.5 Broadcast Address

The address with the host part bits set to 1 is the broadcast address, meaning for every station.

Network and broadcast addresses must not be used as a host address (for example, 192.168.0.0 identifies the entire network and 192.168.0.255 identifies the broadcast address).

10.6 IP Netmask

The netmask is used to divide the IP address differently from the standard defined by classes A, B, C. A netmask defines how many bits from the IP address are to be taken as the network section and how many bits are to be taken as the host section. When the number of host bits is entered, the CoBox-FL calculates the netmask. The netmask is displayed in standard decimal-dot notation.

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

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

10.7 Private IP Networks and the Internet

If your network is not connected to the Internet, and there are no plans to make such a connection, you may use any IP address you wish.

If your network is not connected to the Internet and you have plans to connect, or you are connected to the Internet and want to operate your CoBox-FLs on an intranet, use one of the subnetworks below. These network numbers have been reserved for such networks. If you have any questions about IP assignment, consult your Network Administrator.

Class A	10.x.x.x
Class B	172.16.x.x
Class C	192.168.0.x

10.8 Network RFCs

For more information regarding IP addressing see the following documents. These can be located on the World Wide Web using one of the directories or indices:

RFC 950 Internet Standard Subnetting Procedure

RFC 1700 Assigned Numbers

RFC 1117 Internet Numbers

RFC 1597 Address Allocation for Private Internets

11. Glossary

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.

AutoIP

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 169.254.255.254) has been explicitly reserved for AutoIP-enabled devices. The range of AutoIP addresses is not to be used over the Internet.

Auto-Negotiate:

Clause 28 of the IEEE 802.3u standard specifies a MAC sublayer 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.

AUI:

Attachment Unit Interface. A 15-pin shielded, twisted pair Ethernet cable used (optionally) to connect between network devices and a MAU.

Autobaud:

Automatic determination and matching of transmission speed.

Backbone:

The main cable in a network.

Bandwidth on Demand:

Feature that allows a remote access device to initiate a second connection to a particular site to increase the amount of data transferred to that site to increase the desired threshold. The network manager configuring the remote access server will specify a number of bits or a percentage of connection bandwidth threshold which will trigger the secondary connection. Multilink PPP is an emerging standard to allow this feature to be interoperable, but right now the only way to ensure correct operation is to use devices on both end from the same vendor.

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.

Binary:

Characteristic of having only two states, such as current on and current off. The binary number system uses only ones and zeros.

Bit:

The smallest unit of data processing information. A bit (or binary digit) assumes the value of either 1 or 0.

Block

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

BNC:

A standardized connector used with Thinnet and coaxial cable.

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.

Broadband:

A data transmission technique allowing multiple high-speed signals to share the bandwidth of a single cable via frequency division multiplexing.

Broadband Network:

A network that uses multiple carrier frequencies to transmit multiplexed signals on a single cable. Several networks may coexist on a single cable without interfering with one another.

Brouter:

A device that routes specific protocols, such as TCP/IP and IPX, and bridges other protocols, thereby combining the functions of both routers and bridges.

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.

CHAP:

(Challenge Handshake Authentication Protocol) Authentication scheme for PPP where the password not only is required to begin connection but also is required during the connection - failure to provide correct password during either login or challenge mode will result in disconnect.

Coaxial Cable:

An electrical cable with a solid wire conductor at its center surrounded by insulating materials and an outer metal screen conductor with an axis of curvature coinciding with the inner conductor - hence "coaxial." Examples are standard Ethernet cable and Thinwire Ethernet cable.

Collision:

The result of two network nodes transmitting on the same channel at the same time. The transmitted data is not usable.

Collision Detect:

A signal indicating that one or more stations are contending with the local station's transmission. The signal is sent by the Physical layer to the Data Link layer on an Ethernet/IEEE 802.3 node.

Communication Server:

A dedicated, standalone system that manages communications activities for other computers.

Cut-through:

Technique for examining incoming packets whereby an Ethernet switch looks only at the first few bytes of a packet before forwarding or filtering it. This process is faster than looking at the whole packet, but it also allows some bad packets to be forwarded.

CSMA/CD:

Carrier Sense Multiple Access with Collision Detection is the Ethernet media access method. All network devices contend equally for access to transmit. If a device detects another device's signal while it is transmitting, it aborts transmission and retries after a brief pause.

Data Link:

A logical connection between two nodes on the same circuit.

Data Link Layer:

Layer 2 of the seven-layer OSI reference model for communication between computers on networks. This layer defines protocols for data packets and how they are transmitted to and from each network device. It is a medium-independent, link-level communications facility on top of the Physical layer, and is divided into two sublayers: medium-access control (MAC) and logical-link control (LLC).

DHCP

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.

Dynamic addressing simplifies network administration because the software keeps track of IP addresses rather than requiring an administrator to manage the task. This means that a new computer can be added to a network without the hassle of manually assigning it a unique IP address. Many ISPs use dynamic IP addressing for dial-up users.

DHCP client support is built into Windows 95 and NT workstation. NT 4 server includes both client and server support.

Dial on Demand:

When a router detects the need to initiate a dial-up connection to a remote network, it does so automatically according to pre-defined parameters set by the network manager.

Dialback:

A security feature that ensures people do not log into modems that they shouldn't have access to. When a connection is requested, the system checks the user name for validity, then "dials back" the number associated with that user name.

Distributed Processing:

A system in which each computer or node in the network performs its own processing and manages some of its data while the network facilitates communications between the nodes.

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.

FDDI:

Fiberoptic Data Distribution Interface. A cable interface capable of transmitting data at 100 Mbps. Originally specified for fiber lines, FDDI can also operate over twisted-pair cable for short distances.

Fiber-Optic Cable:

A transmission medium composed of a central glass optical fiber cable surrounded by cladding and an outer protective sheath. It transmits digital signals in the form of modulated light from a laser or LED (light-emitting diode).

File Server:

A computer that stores data for network users and provides network access to that data.

Filtering:

Process whereby an Ethernet switch or bridge reads the contents of a packet and then finds that the packet does not need to be forwarded, drops it. a filtering rate is the rate at which a device can receive packets and drop them without any loss of incoming packets or delay in processing.

Firmware:

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

Forwarding:

Process whereby an Ethernet switch or bridge reads the contents of a packet and then passes that packet on to the appropriate attached segment. A forwarding rate is the time that it takes the device to execute all of the steps.

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.

Header:

The initial part of a data packet or frame containing identifying information such as the source of the data, its destination, and length.

Heartbeat:

Ethernet defined SQE signal quality test function.

Hertz (Hz):

A frequency unit equal to one cycle per second.

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.

HTTP

Short for HyperText Transfer Protocol, the underlying protocol used by the World Wide Web. HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands. For example, when you enter a URL in your browser, this actually sends an HTTP command to the Web server directing it to fetch and transmit the requested Web page.

HTTP is called a stateless protocol because each command is executed independently, without any knowledge of the commands that came before it. This is the main reason that it is difficult to implement Web sites that react intelligently to user input. This shortcoming of HTTP is being addressed in a number of new technologies, including ActiveX, Java, JavaScript and cookies.

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.

IPX:

Internetwork Packet eXchange, a NetWare protocol similar to IP (Internet Protocol).

ISDN:

(Integrated Services Digital Network): All digital service provided by telephone companies. Provides 144K bps over a single phone line (divided in two 64K bps "B" channels and one 16K bps "D" channel).

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.

Jabber:

Network error caused by an interface card placing corrupted data on the network. Or, an error condition due to an Ethernet node transmitting longer packets than allowed.

Kbps:

Kilobits per second.

Kermit:

A popular file transfer and terminal emulation program.

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.

LAT:

Local Area Transport, a Digital Equipment Corporation proprietary network communication protocol. The protocol is based on the idea of a relatively small, known number of hosts on a local network sending small network packets at regular intervals. LAT will not work on a wide area network scale, as TCP/IP does.

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.

Local Network Interconnect (LNI):

A Port Multiplier, or concentrator supporting multiple active devices or communications controllers, either used standalone or attached to standard Ethernet cable.

Logical Link:

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

MAU:

Medium Attachment Unit, a device used to convert signals from one Ethernet medium to another.

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.

MII:

Media Independent Interface, New standard developed for Fast Ethernet in IEEE 802.3u specification. The Fast Ethernet equivalent to the AUI in 10 Mbps Ethernet, allowing different types of Fast Ethernet media to be connected to a Fast Ethernet device via a common interface.

MJ:

Modular Jack. A jack used for connecting voice cables to a faceplate, as for a telephone.

MMJ:

Modified Modular Jack. These are the 6-pin connectors used to connect serial terminal lines to terminal devices. MMJs can be distinguished from the similar RJ12 jacks by having a side-locking tab, rather than a center-mounted one.

Modem:

A modulator-demodulator device for changing transmission signals from digital to analog for transmission over phone lines. Used in pairs, one is required at each end of the line.

MOP:

Maintenance Operations Protocol, a DEC protocol used for remote communications between hosts and servers.

Multicast:

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

Multilink PPP:

The ability of a dialup device to allocate more than one channel of bandwidth to a particular connection. Generally, this is termed to be the ability of an ISDN device to bond two B-channels together into a single data pipe, but some vendors can perform the same function with asychronous dial-up connections over modems by having a second connection initiated to support the additional bandwidth requirements.

Multiplexer:

A device that allows several users to share a single circuit. It funnels different data streams into a single stream. At the other end of the communications link, another multiplexer reverses the process by splitting the data stream back into the original streams.

Multiplexing:

Transmitting multiple signals simultaneously on a single channel.

Multiport Repeater:

A repeater, either standalone or connected to standard Ethernet cable, for interconnecting up to eight Thinwire Ethernet segments.

Name Server:

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

NetWare:

A Novell developed Network Operating System (NOS). Provides file and printer sharing among networks of Personal Computers (PCs). Each NetWare network must have at least one file server, and access to other resources is dependent on connecting to and logging into the file server. The file server controls user logins and access to other network clients, such as user PCs, print servers, modem/fax servers, disk/file servers, etc.

NetBIOS/NetBEUI:

Microsoft's networking protocols for it's LAN Manager and Windows NT products.

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.

NIC:

Network Interface Card, an adapter card that is inserted into a computer, and contains the necessary software and electronics to enable the station to communicate over the network.

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."

NOS:

Network Operating System, the software for a network that runs in a file server and controls access to files and other resources from multiple users. It provides security and administrative tools. Novell's NetWare, Banyan's VINES and IBM's LAN Server are NOS examples.

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.

PAP:

(Password Authentication Protocol) Authentication scheme for PPP links. A password can be specified for both devices on a remote link. Failure to authenticate will result in a dropped connection prior to start of data transmission.

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.

Point-to-Point:

A circuit connecting two nodes only, or a configuration requiring a separate physical connection between each pair of nodes.

Port:

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

Port Multiplier:

A concentrator providing connection to a network for multiple devices.

PostScript:

A printer/display protocol developed by Adobe Corp. PostScript is an actual printing and programming language to display text and graphics. Unlike line/ASCII printers, which print character input verbatim, PostScript printers accept and interpret an entire PostScript page before printing it.

PPP:

Point-to-Point Protocol. The successor to SLIP, PPP provides router-to-router and host-to-network connections over both synchronous and asynchronous circuits.

Print Server:

A dedicated computer that manages printers and print requests from other nodes on the network.

PROM:

Programmable ROM, a read-only memory whose data content can be altered.

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.)

Remote Control:

Form of remote access where a device dialing in assumes control of another network node - all keystrokes on the remote are translated into keystrokes on the network node. Used primarily with IPX protocol.

Remote Node:

Form of remote access where the device dialing in acts as a peer on the target network. Used with both IP and IPX protocols.

Repeater:

A repeater is a network device that repeats signals from one cable onto one or more other cables, while restoring signal timing and waveforms.

Ring:

A network topology in which the nodes are connected in a closed loop. Data is transmitted from node to node around the loop, always in the same direction.

RMON:

SNMP-based standard for reporting various network conditions. RMON has 10 different management groups which provide detailed information about a network.

Rlogin:

Rlogin is an application that provides a terminal interface between UNIX hosts using the TCP/IP network protocol. Unlike Telnet, Rlogin assumes the remote host is (or behaves like) a UNIX machine

ROM:

Read-Only Memory, a memory device that retains its information even when power to it is removed. A ROM version of a network device does not need to download, since the ROM contains the entire executable code and thus never needs to reload it. Frequently the ROM is provided as "flash ROM", which can be reprogrammed by downloading if the user chooses.

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.

RTEL:

Lantronix' "reverse Telnet" software allows hosts using TCP/IP to establish a session with a device attached to a terminal server port.

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.

Shared Ethernet:

Ethernet configuration in which a number of segments are bound together in a single collision domain. Hubs produce this type of configuration where only one node can transmit at a time.

SLIP:

Serial Line Internet Protocol, a protocol for running TCP/IP over serial lines.

SNA:

Systems Network Architecture. IBM's layered protocols for mainframe communications.

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.

Spanning Tree:

An algorithm used by bridges to create a logical topology that connects all network segments, and ensures that only one path exists between any two stations.

Store and Forward:

Technique for examining incoming packets on an Ethernet switch or bridge whereby the whole packet is read before forwarding or filtering takes place. Store and forward is a slightly slower process than cut-through, but it does ensure that all bad or misaligned packets are eliminated from the network by the switching device.

SPX:

Sequential Packet exchange. Novell's implementation of SPP (Sequential Packet Protocol).

SQE:

Ethernet-defined signal quality test function, frequently called "heartbeat."

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.

T-Connector:

A T-shaped device with two female and one male BNC connectors.

TCP/IP:

Transmission Control Protocol (TCP) and Internet Protocol (IP) are the standard network protocols in UNIX environments. They are almost always implemented and 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.

10BASE2:

Ethernet running on thin coax network cable.

10BASE5:

Ethernet running on Thickwire network cable.

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.

Terminal Server:

A concentrator that facilitates communication between hosts and terminals.

Terminator:

Used on both ends of a standard Ethernet or Thinwire Ethernet segment, this special connector provides the 50 ohm termination resistance needed for the cable.

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.

Thickwire:

Half-inch diameter coax cable.

Thinwire:

Thin coaxial cable similar to that used for television/video hookups.

Throughput:

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

Token:

The character sequence or frame, passed in sequence from node to node, to indicate that the node controlling it has the right to transmit for a given amount of time.

Token Ring:

Developed by IBM, this 4 or 16 Mbps network uses a ring topology and a token-passing access method.

Topology:

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

Transceiver:

The actual device that interfaces between the network and the local node. The term generally refers to any connector, such as a MAU, that actively converts signals between the network and the local node.

Transceiver Cable:

Cable that attaches a device either to a standard or thin coax Ethernet segment.

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.

Unix:

A multitasking, multiuser computer operating system developed by AT&T. Several versions exist, e.g., the Berkeley version.

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.

Workgroup Switching:

Configuration in which a number of users are connected to an Ethernet network via a switch. Switching allows each user to get greater throughput than would be available through a hub.

X.25 Gateway Access Protocol:

Allows a node not directly connected to a public data network to access the facilities of that network through an intermediary gateway node. X.25 is the protocol standard governing packet-switched networks.

Artisan Technology Group is an independent supplier of quality pre-owned equipment

Gold-standard solutions

Extend the life of your critical industrial, commercial, and military systems with our superior service and support.

We buy equipment

Planning to upgrade your current equipment? Have surplus equipment taking up shelf space? We'll give it a new home.

Learn more!

Visit us at **artisantg.com** for more info on price quotes, drivers, technical specifications, manuals, and documentation.

Artisan Scientific Corporation dba Artisan Technology Group is not an affiliate, representative, or authorized distributor for any manufacturer listed herein.

We're here to make your life easier. How can we help you today?

(217) 352-9330 | sales@artisantg.com | artisantg.com

ARTISAN® TECHNOLOGY GROUP