



## EDS Device Servers User Guide

- ◆ EDS4100
- ◆ EDS8PR
- ◆ EDS16PR
- ◆ EDS32PR

## Copyright & Trademark

© 2006, 2007 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.

## Contacts

### Lantronix Corporate Headquarters

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

### Technical Support

Online: [www.lantronix.com/support](http://www.lantronix.com/support)

### Sales Offices

For a current list of our domestic and international sales offices, go to the Lantronix web site at [www.lantronix.com/about/contact](http://www.lantronix.com/about/contact).

## Disclaimer & Revisions

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

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

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

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

Date	Rev.	Comments
3/06	A	Initial Document
10/06	B	EDS16PR and EDS32PR products added.
12/06	D	German and English TUV certification added.
1/07	E	EDS8PR products added.

# Contents

<b>1: Preface</b>	<b>10</b>
Purpose and Audience _____	10
Summary of Chapters _____	10
Additional Documentation _____	11
<b>2: Introduction</b>	<b>12</b>
EDS4100 Overview _____	12
Features _____	13
EDS8PR, EDS16PR and EDS32PR Overview _____	13
Features _____	14
Evolution OS™ _____	14
Web-Based Configuration and Troubleshooting _____	15
Command-Line Interface (CLI) _____	15
SNMP Management _____	15
XML-Based Architecture and Device Control _____	15
Rich Site Summary (RSS) _____	15
Enterprise-Grade Security _____	15
Troubleshooting Capabilities _____	16
Applications _____	17
Building Automation/Security _____	17
Industrial Automation _____	17
Medical/Healthcare _____	17
Retail Automation/Point-of-Sale _____	18
Console Management _____	18
Traffic Management _____	18
<b>3: Installation: EDS4100</b>	<b>19</b>
Package Contents _____	19
User-Supplied Items _____	19
Identifying Hardware Components _____	20
Serial Ports _____	21
Ethernet Port _____	22
Terminal Block Connector _____	22
LEDs _____	22
Reset Button _____	23
Physically Installing the EDS4100 _____	23

Finding a Suitable Location _____	23
Connecting the EDS4100 _____	23
<b>4: Installation: EDS8PR, EDS16PR and EDS32PR</b>	<b>25</b>
Package Contents _____	25
User-Supplied Items _____	25
Identifying Hardware Components _____	26
Serial Ports _____	27
Ethernet Port _____	27
LEDs _____	27
Reset Button _____	28
Physically Installing the EDS8/16/32PR _____	28
Finding a Suitable Location _____	28
Connecting the EDS8/16/32PR _____	28
<b>5: Getting Started</b>	<b>30</b>
Using DeviceInstaller _____	30
Starting DeviceInstaller _____	30
Viewing EDS Properties _____	31
Configuration Methods _____	32
Configuring from the Web Manager Interface _____	32
Configuring via an SSH/Telnet Session or Serial Port Using the CLI _____	32
Configuring from the XML Interface _____	33
<b>6: Configuration Using the Web Manager</b>	<b>34</b>
Accessing the Web Manager through a Web Browser _____	34
Navigating Through the Web Manager _____	36
Understanding the Web Manager Pages _____	42
Device Status Page _____	43
<b>7: Network, Serial Line, and Tunnel Settings</b>	<b>44</b>
Network Configuration Page _____	44
Line Settings Pages _____	47
Line – Statistics Page _____	48
Line - Configuration Page _____	49
Line – Command Mode Page _____	51
Tunnel Pages _____	52
Tunnel – Statistics Page _____	52
Tunnel – Serial Settings Page _____	53
Tunnel – Start/Stop Characters Page _____	55
Tunnel – Accept Mode Page _____	56

Tunnel – Connect Mode Page _____	59
Tunnel – Disconnect Mode Page _____	62
Tunnel – Packing Mode Page _____	64
Tunnel – Modem Emulation Page _____	65
Tunnel – AES Keys Page _____	67
<b>8: Services Settings</b>	<b>70</b>
DNS Page _____	70
SNMP Page _____	71
FTP Page _____	72
TFTP Page _____	74
Syslog Page _____	75
HTTP Pages _____	76
HTTP Statistics Page _____	76
HTTP Configuration Page _____	77
HTTP Authentication Page _____	79
HTTP RSS Page _____	82
<b>9: Security Settings</b>	<b>84</b>
SSH Pages _____	84
SSH Server: Host Keys Page _____	84
SSH Client: Known Hosts Page _____	86
SSH Server: Authorized Users Page _____	88
SSH Client: Users Page _____	89
SSL Page _____	92
<b>10: Maintenance and Diagnostics Settings</b>	<b>95</b>
Filesystem Pages _____	95
Filesystem Statistics Page _____	95
Filesystem Browser Page _____	96
Diagnostics Pages _____	98
Diagnostics: Hardware Page _____	98
MIB-II Network Statistics Page _____	99
IP Sockets Page _____	100
Diagnostics: Ping Page _____	101
Diagnostics: Traceroute Page _____	102
Diagnostics: DNS Lookup Page _____	103
Diagnostics: Memory Page _____	104
Diagnostics: Buffer Pool _____	105
Diagnostics: Processes Page _____	106
System Page _____	107

Query Port Page _____	109
<b>11: Advanced Settings</b>	<b>111</b>
Email Pages _____	111
Email Statistics Page _____	111
Email Configuration Page _____	112
CLI Pages _____	114
Command Line Interface Statistics Page _____	114
Command Line Interface Configuration Page _____	115
XML Pages _____	117
XML Configuration Record: Export System Configuration Page _____	117
XML Status Record: Export System Status _____	119
XML: Import System Configuration Page _____	120
Protocol Stack Page _____	122
IP Address Filter Page _____	124
<b>12: Updating Firmware</b>	<b>126</b>
Obtaining Firmware _____	126
Upgrading Using DeviceInstaller _____	126
Loading New Firmware _____	126
Updating the Boot Loader from DeviceInstaller _____	126
Updating Firmware _____	127
<b>A: Factory Default Configuration</b>	<b>128</b>
Network Configuration Settings _____	128
Serial Port Line Settings _____	128
Tunnel Settings _____	129
Serial Settings _____	129
Start/Stop Characters _____	129
Accept Mode _____	130
Connect Mode _____	130
Disconnect Mode _____	131
Packing Mode _____	131
Modem Emulation _____	131
AES Keys _____	132
DNS Settings _____	132
SNMP Settings _____	132
FTP Settings _____	133
TFTP Settings _____	133
Syslog Settings _____	133

HTTP Settings _____	134
Configuration _____	134
Authentication _____	134
RSS _____	134
CLI Settings _____	135
Telnet _____	135
Email Settings _____	135
Query Port Settings _____	136
Diagnostics Settings _____	136
Ping _____	136
System Settings _____	136
IP Address Filter _____	136
<b>B: Technical Specifications</b>	<b>137</b>
EDS4100 _____	137
EDS8/16/32PR _____	139
<b>C: Networking and Security</b>	<b>141</b>
SSL _____	141
Benefits of SSL _____	141
How SSL Works _____	142
Digital Certificates _____	142
SSH _____	143
How Does SSH Authenticate? _____	143
What Does SSH Protect Against? _____	143
Tunneling _____	144
Tunneling and the EDS _____	145
Connect Mode _____	145
Accept Mode _____	146
Disconnect Mode _____	146
Packing Mode _____	147
Modem Emulation _____	147
Command Mode _____	148
<b>D: Technical Support</b>	<b>150</b>
<b>E: Lantronix Cables and Adapters</b>	<b>151</b>
<b>F: Compliance</b>	<b>152</b>
Lithium Battery Notice _____	153
Installationsanweisungen _____	153
Rackmontage _____	153

Energiezufuhr _____	153
Erdung _____	153
Installation Instructions _____	153
Rack Mounting _____	153
Input Supply _____	154
Grounding _____	154
<b>G: Warranty</b>	<b>155</b>
<b>Index</b>	<b>156</b>

## Figures

Figure 2-1. EDS4100 4 Port Device Server.....	13
Figure 2-2. EDS16PR Device Server.....	14
Figure 3-1. Front View of the EDS4100.....	20
Figure 3-2. Back View of the EDS4100.....	20
Figure 3-3. RS-232 Serial Port Pins (Serial Ports 1, 2, 3, 4).....	21
Figure 3-4. RS-422/RS-485 Serial Port Pins.....	21
Figure 3-5. Terminal Block Connector Pin Assignments.....	22
Figure 3-6. Back Panel LEDs.....	22
Figure 3-7. Example of EDS4100 Connections.....	24
Figure 4-1. Front View of the EDS16PR.....	26
Figure 4-2. Back View of the EDS16PR.....	26
Figure 4-3. RJ45 Serial Port.....	27
Figure 4-4. Example of EDS16PR Connections.....	29
Figure 5-1. Lantronix DeviceInstaller.....	30
Figure 5-2. EDS4100 Properties.....	31
Figure 6-1. Prompt for User Name and Password.....	34
Figure 6-2. Web Manager Device Status Page.....	35
Figure 6-3. Web Manager Menu Structure (1 of 4).....	38
Figure 6-4. Web Manager Menu Structure (2 of 4).....	39
Figure 6-5. Web Manager Menu Structure (3 of 4).....	40
Figure 6-6. Web Manager Menu Structure (4 of 4).....	41
Figure 6-7. Components of the Web Manager Page.....	42
Figure 6-8. Device Status Page (EDS4100).....	43
Figure 7-1. Network Configuration.....	45
Figure 7-2. Line –Statistics Page.....	48
Figure 7-3. Configuration Page.....	49
Figure 7-4. Line – Command Mode Page.....	51
Figure 7-5. Tunnel - Statistics Page.....	53
Figure 7-6. Tunnel – Serial Settings Page.....	54
Figure 7-7. Tunnel – Start/Stop Chars Page.....	55
Figure 7-8. Tunnel – Accept Mode Page.....	57
Figure 7-9. Connect Mode Page.....	60
Figure 7-10. Tunnel – Disconnect Mode Page.....	63
Figure 7-11. Tunnel – Packing Mode Page.....	64
Figure 7-12. Tunnel – AES Keys Page.....	68
Figure 8-1. DNS Page.....	70
Figure 8-2. SNMP Page.....	71
Figure 8-3. FTP Page.....	73
Figure 8-4. TFTP Page.....	74



Figure 8-5. Syslog Page .....	75
Figure 8-6. HTTP Statistics Page .....	76
Figure 8-7. HTTP Configuration Page .....	77
Figure 8-8. HTTP Authentication Page .....	80
Figure 8-9. HTTP RSS Page .....	82
Figure 9-1. SSH Server: Host Keys Page .....	85
Figure 9-2. SSH Client: Known Hosts Page .....	87
Figure 9-3. SSH Server: Authorized Users Page .....	88
Figure 9-4. SSH Client: Users Page .....	90
Figure 9-5. SSL Page .....	93
Figure 10-1. Filesystem Statistics Page .....	95
Figure 10-2. Filesystem Browser Page .....	96
Figure 10-3. MIB-II Network Statistics Page .....	99
Figure 10-4. IP Sockets Page .....	100
Figure 10-5. Diagnostics: Ping Page .....	101
Figure 10-6. Diagnostics: Traceroute Page .....	102
Figure 10-7. Diagnostics: DNS Lookup Page .....	103
Figure 10-8. Diagnostics: Memory Page .....	104
Figure 10-9. Diagnostics: Buffer Pools Page .....	105
Figure 10-10. Diagnostics: Processes Page .....	106
Figure 10-11. System Page .....	108
Figure 10-12. Query Port Page .....	110
Figure 11-1. Email Statistics Page .....	112
Figure 11-2. Email Configuration Page .....	113
Figure 11-3. Command Line Interface Statistics Page .....	115
Figure 11-4. Command Line Interface Configuration Page .....	116
Figure 11-5. XML Configuration Record: Export System Configuration Page .....	118
Figure 11-6. XML Status Record: Export System Status Page .....	119
Figure 11-7. XML: Import System Configuration Page .....	121
Figure 11-8. Protocol Stack Page .....	123
Figure 11-9. IP Address Filter Page .....	125

# 1: Preface

## Purpose and Audience

This guide describes how to install, configure, use, and update the EDS4100 4-Port, EDS8PR 8-Port, EDS16PR 16-Port, and EDS32PR 32-Port Device Servers. It is for users who will use the EDS to network-enable their serial devices.

## Summary of Chapters

The remaining chapters in this guide include:

Chapter	Description
<a href="#">2: Introduction</a>	Main features of the EDS device servers and the applications for which they are suited.
<a href="#">3: Installation: EDS4100</a>	Instructions for getting the EDS4100 device server up and running. Includes a description of hardware components.
<a href="#">4: Installation: EDS8PR, EDS16PR and EDS32PR</a>	Instructions for getting the EDS8PR, EDS16PR and EDS32PR device server up and running. Includes a description of hardware components.
<a href="#">5: Getting Started</a>	Instructions for starting DeviceInstaller and viewing current configuration settings. Introduces methods of configuring the EDS.
<a href="#">6: Configuration Using the Web Manager</a>	Instructions for using the web interface to configure EDS device servers.
<a href="#">7: Network, Serial Line, and Tunnel Settings</a>	Instructions for using the web interface to configure network, serial line, and tunnel settings.
<a href="#">8: Services Settings</a>	Instructions for using the web interface to configure settings for DNS, SNMP, FTP, and other services.
<a href="#">9: Security Settings</a>	Instructions for using the web interface to configure SSH and SSL security settings.
<a href="#">10: Maintenance and Diagnostics</a>	Instructions for using the web interface to maintain the EDS, view statistics, files, and logs, and diagnose problems.
<a href="#">11: Advanced Settings</a>	Instructions for using the web interface to configure advanced settings, e.g., email, CLI, and XML.
<a href="#">12: Updating Firmware</a>	Instructions for upgrading the EDS firmware.

Chapter	Description
<i>A: Factory Default Configuration</i>	Quick reference of the EDS factory-default configuration settings.
<i>B: Technical Specifications</i>	Tables of technical data about the products...
<i>C: Networking and Security</i>	In-depth description of networking and network security as it relates to the EDS device servers.
<i>D: Technical Support</i>	Information about contacting Lantronix Technical Support.
<i>F: Compliance</i>	Information about the products' compliance with regulatory standards.
<i>G:Warranty</i>	Provides information on the Lantronix warranty for the EDS.

## Additional Documentation

The following guide is available on the product CD or the Lantronix Web site:  
[www.lantronix.com](http://www.lantronix.com).

Document	Description
<b>EDS Device Server Quick Start Guide</b>	Provides the steps for getting the EDS up and running.
<b>EDS Device Server Command Reference</b>	Describes how to configure the EDS using Telnet or the serial port and summarizes the CLI and XML configuration commands.
<b>Secure Com Port Redirector User Guide</b>	Provides information for using the Lantronix Windows-based utility to create secure virtual com ports.

## 2: Introduction

This chapter introduces the Lantronix EDS family of device servers. It provides an overview of the products, lists their key features, and describes the applications for which they are suited.

EDS device servers contain all the components necessary to deliver full network connectivity to virtually any kind of serial device, a reliable TCP/IP protocol stack, and a variety of remote management capabilities. They boast an innovative design and run on Lantronix's leading-edge Evolution OS™.

### EDS4100 Overview

The EDS4100 is a compact, easy-to-use device server that gives you the ability to network-enable asynchronous RS-232 and RS-422/485 serial devices. It can deliver fully transparent RS-232/422 point-to-point connections and RS-485 multi-drop connections without requiring modifications to existing software or hardware components in your application.

**Note:** RS-485 circuits support 32 full-load devices or 128 quarter-load devices. Each EDS4100 RS-485 port, however, counts as one device, leaving up to 31 full-load or 127 quarter-load devices that can be connected to the RS-485 circuit.

*The EDS4100 device server supports the Power-over-Ethernet (PoE) standard. With PoE, power is supplied to the EDS over the Ethernet cable, by either an Ethernet switch or a midspan device. Being able to draw power through the Ethernet cable eliminates power supply and cord clutter. It also allows the EDS to be located in areas where power is not typically available.*

- ◆ Ports 1 through 4 support RS-232 devices.
- ◆ Ports 1 and 3 also support RS-422/485 devices.

Figure 2-1. EDS4100 4 Port Device Server



## Features

The following list summarizes the key features of the EDS4100.

- ◆ Includes four serial ports with hardware handshaking signals
- ◆ Supports RS-232 and RS-422/485
- ◆ Includes one RJ45 Ethernet port
- ◆ Supports the IEEE 802.3af standard for Power-over-Ethernet (PoE)
- ◆ 8 MB Flash memory
- ◆ 32 MB Random Access Memory (RAM)
- ◆ Based on Lantronix's Evolution OS™
- ◆ Supports secure data encryption by means of AES, SSH, or SSL sessions
- ◆ Supports three convenient configuration methods (Web, command line, and XML)

## EDS8PR, EDS16PR and EDS32PR Overview

The EDS8PR (8 serial ports), EDS16PR (16 serial ports), and EDS32PR (32 serial ports) are compact easy-to-use, rack-mountable device servers that give you the ability to network-enable asynchronous RS-232 serial devices. They provide fully transparent RS-232 point-to-point connections without requiring modifications to existing software or hardware components in your application.

Figure 2-2. EDS16PR Device Server



## Features

The following list summarizes the key features of the EDS8PR,, EDS16PR and EDS32PR.

- ◆ Includes 8 (EDS8PR), 16 (EDS16PR) or 32 (EDS32PR) serial ports with hardware handshaking signals
- ◆ Supports RS-232
- ◆ Includes one RJ45 Ethernet port
- ◆ 8 MB Flash memory
- ◆ 32 MB Random Access Memory (RAM)
- ◆ Based on Lantronix's Evolution OS™
- ◆ Includes a dedicated console port
- ◆ Supports secure data encryption by means of AES, SSH, or SSL sessions
- ◆ Supports three convenient configuration methods (Web, command line, and XML)

## Evolution OS™

EDS device servers incorporate Lantronix's Evolution OS™. Key features of the Evolution OS™ include:

- ◆ Built-in Web server for configuration and troubleshooting from Web-based browsers
- ◆ CLI configurability
- ◆ SNMP management
- ◆ XML data transport and configurability
- ◆ Rich Site Summary (RSS) information feeds
- ◆ Enterprise-grade security with SSL and SSH
- ◆ Comprehensive troubleshooting tools

## Web-Based Configuration and Troubleshooting

Built upon popular Internet-based standards, the EDS enables users to configure, manage, and troubleshoot efficiently through a simplified browser-based interface that can be accessed anytime from anywhere. All configuration and troubleshooting options are launched from a well-organized, multi-page interface. Users can access all functionality via a Web browser, allowing them flexibility and remote access. As a result, users can enjoy the twin advantages of decreased downtime (based on the troubleshooting tools) and the ability to implement configuration changes easily (based on the configuration tools).

In addition, users can load their own Web pages onto the EDS to facilitate monitoring and control of their own serial devices that are attached to the EDS.

## Command-Line Interface (CLI)

Making the edge-to-enterprise vision a reality, the EDS with the Evolution OS™ uses industry-standard tools for configuration, communication, and control. For example, the Evolution OS™ uses a Cisco®-like command line interface (CLI) whose syntax is very similar to that used by data center equipment such as routers and hubs.

## SNMP Management

The EDS supports full SNMP management, making it ideal for applications where device management and monitoring are critical. These features allow networks with SNMP capabilities to correctly diagnose and monitor EDS device servers.

## XML-Based Architecture and Device Control

XML is a fundamental building block for the future growth of M2M networks. The EDS supports XML-based configuration setup records that makes device configuration transparent to users and administrators. The XML is easily editable with a standard text or XML editor.

## Rich Site Summary (RSS)

The EDS supports Rich Site Summary (RSS), a rapidly emerging technology for streaming and managing on-line content. RSS feeds all the configuration changes that occur on the device. The feed is then read (polled) by an RSS aggregator. More powerful than simple email alerts, RSS uses XML as an underlying Web page transport and adds intelligence to the networked device while not taxing already overloaded email systems.

## Enterprise-Grade Security

Without the need to disable any features or functionality, the Evolution OS™ provides the EDS the highest level of security possible. This 'data center grade' protection ensures that each device on the M2M network carries the same level of security as traditional IT networking equipment in the corporate data center.

With built-in SSH and SSL, secure communications can be established between the EDS serial ports and the remote end device or application. By protecting the privacy of serial data being transmitted across public networks, users can maintain their existing

investment in serial technology, while taking advantage of the highest data-protection levels possible.

SSH and SSL can:

- ◆ Verify the data received came from the proper source
- ◆ Validate that the data transferred from the source over the network has not changed when it arrives at its destination (shared secret and hashing)
- ◆ Encrypt data to protect it from prying eyes and nefarious individuals
- ◆ Provide the ability to run popular M2M protocols over a secure SSH connection

In addition to keeping data safe and accessible, the EDS has robust defenses to hostile Internet attacks such as denial of service (DoS), which can be used to take down the network. Moreover, the EDS can not be used to bring down other devices on the network.

The EDS can be used with Lantronix's Secure Com Port Redirector (SCPR) to encrypt COM port-based communications between PCs and virtually any electronic device. SCPR is a Windows application that creates a secure communications path over a network between the computer and serial-based devices that are traditionally controlled via a COM port. With SCPR installed at each computer, computers that were formerly "hard-wired" by serial cabling for security purposes or to accommodate applications that only understood serial data can instead communicate over an Ethernet network or the Internet.

The EDS also supports a variety of popular cipher technologies including:

- ◆ Advanced Encryption Standard (AES)
- ◆ Triple Data Encryption Standard (3DES)
- ◆ RC4
- ◆ Hashing algorithms such as Secure Hash Algorithm (SHA-1) and MD5

## Troubleshooting Capabilities

The EDS offers a comprehensive diagnostic toolset that lets you troubleshoot problems quickly and easily. Available from the Web Manager, CLI, and XML interfaces, the diagnostic tools let you:

- ◆ View critical hardware, memory, MIB-II, buffer pool, and IP socket information.
- ◆ Perform ping and traceroute operations.
- ◆ Conduct forward or backup DNS lookup operations.
- ◆ View all processes currently running on the EDS, including CPU utilization and total stack space available.



## Applications

EDS device servers deliver simple, reliable, and cost-effective network connectivity for all your serial devices and address the growing need to connect individual devices to the network over industry-standard Ethernet connections. The EDS is ideal for a variety of applications, including:

- ◆ Building automation/security
- ◆ Industrial automation
- ◆ Medical/healthcare
- ◆ Retail automation/point-of-sale
- ◆ Console management
- ◆ Traffic management

### Building Automation/Security

Automating, managing, and controlling many different aspects of a building is possible with the EDS. It can overcome the hurdle of stand-alone networks or individual control systems that are not able to communicate with each other, and not able to share vital data, in a cost effective way.

The EDS can also be used to centrally manage equipment and devices over a new or existing Ethernet network to improve the safety and comfort of building occupants, while lowering heating, ventilating, air conditioning (HVAC), lighting, and overall energy operating costs through centralized management and monitoring.

### Industrial Automation

Today's manufacturing facilities face the common challenges of productivity improvements, inventory management, and quality control. From warehouse to automotive environments, the need to attach the following devices, whether new or legacy, continues to grow:

- ◆ Programmable Logic Controllers (PLCs), Computer Numeric Control and Direct Numeric Control (CNC/DNC) equipment, process and quality-control equipment
- ◆ Pump controllers
- ◆ Bar-code readers and scanners, operator displays, scales, and weighing stations
- ◆ Printers, machine-vision systems, and other types of manufacturing equipment

The EDS is well suited to deliver network connectivity to all of these devices.

### Medical/Healthcare

Hospitals, clinics, and laboratories face rapidly growing needs to deliver medical information accurately, quickly, and easily, whether at bedside, the nurse's station, or anywhere in the facility. The goal to improve healthcare services, however, is balanced with the need to keep the bottom line from exceeding already constrained budgets.

The EDS can network enable medical equipment and devices using the hospital's existing Ethernet network to improve patient care and slash operating costs. This allows

medical staff members to easily monitor and control equipment over the network, whether it is located at the point of care, in a laboratory, or somewhere else in the building, all resulting in improved quality of service and reduced operational costs.

### **Retail Automation/Point-of-Sale**

Having the right solution in the store to manage deliveries, track orders, and keep pricing current are all improvements that the EDS can offer to make retail operations more successful. From big to small, one store to thousands of outlets, the EDS can empower point-of-sale (POS) devices to share information across the network effectively.

With the EDS, retailers can increase and streamline productivity quickly and easily by network-enabling serial devices like card swipe readers, bar-code scanners, scales, cash registers, and receipt printers.

### **Console Management**

Remote offices can have routers, PBXs, servers and other networking equipment that require remote management from the corporate facility. The EDS easily attaches to the serial ports on a server, Private Branch Exchange (PBX), or other networking equipment to deliver central, remote monitoring and management capability.

### **Traffic Management**

With the ubiquity of Ethernet networks, managing cities over Ethernet is now within reach. The EDS provides an easy conversion from serial ports on traffic cameras, billboards, and traffic lights to Ethernet. The EDS obviates the need for long-haul modems and enables the management of traffic equipment over the network.

## 3: Installation: EDS4100

This chapter describes how to install the EDS4100 device server.

### Package Contents

Your EDS4100 package includes the following items:

- ◆ One EDS4100 device server
- ◆ One RJ45-to-DB9Fnull modem cable
- ◆ One product CD that includes this User Guide, the Command Reference, and the Quick Start guide.
- ◆ A printed Quick Start guide

Your package may also include a power supply.

### User-Supplied Items

To complete your EDS4100 installation, you need the following items:

- ◆ RS-232 and/or RS-422/485 serial devices that require network connectivity:
  - Each EDS4100 serial port supports a directly connected RS-232 serial device.
  - Ports 1 and 3 also support RS-422/485 and can accommodate 31 full-load RS-485 multi-drop devices or 127 quarter-load RS-485 multi-drop devices per port, for a total of 62 full-load or 254 quarter-load devices.
- ◆ A serial cable for each serial device to be connected to the EDS4100. One end of the cable must have a female DB9 connector to connect to the EDS4100 serial port. The connector on the other end must be configured for your serial device.

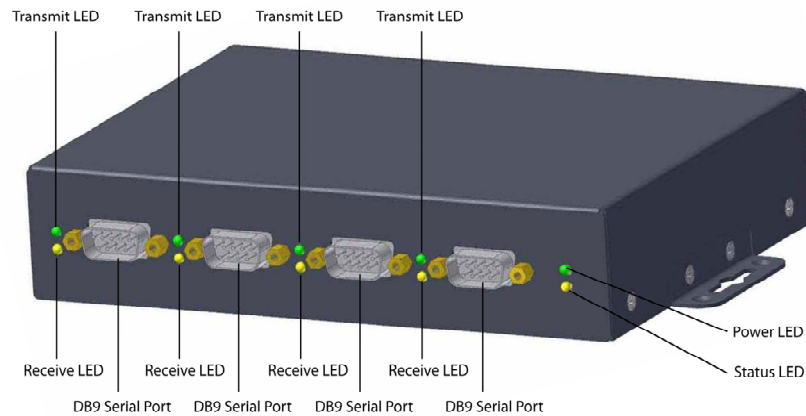
**Note:** To connect an EDS4100 serial port to another DTE device, you will need a null modem cable, such as the one supplied in your EDS4100 package. To connect the EDS4100 serial port to a DCE device, you will need a straight-through (modem) cable.

- ◆ An available connection to your Ethernet network and an Ethernet cable.
- ◆ A working power outlet if the unit will be powered from an AC outlet.

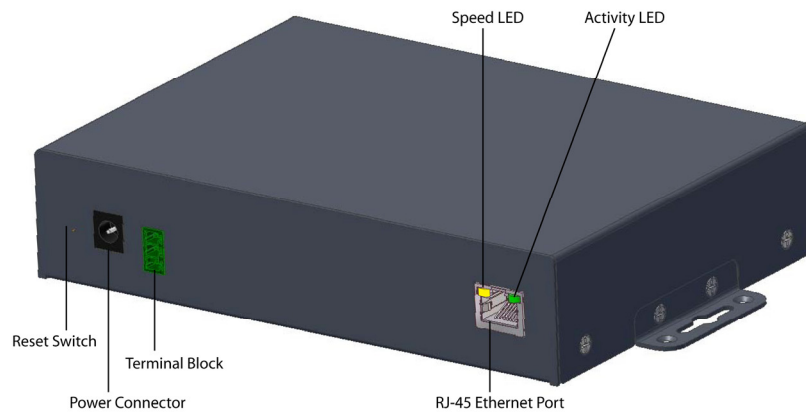
## Identifying Hardware Components

Figure 3-1 shows the hardware components on the front of the EDS4100. Figure 3-2 shows the hardware components on the back of the EDS4100.

**Figure 3-1. Front View of the EDS4100**



**Figure 3-2. Back View of the EDS4100**



The bottom of the EDS4100 (not shown) has a product information label. This label contains the following information:

- ◆ Bar code
- ◆ Serial number
- ◆ Product ID (name)
- ◆ Product description
- ◆ Hardware address (also referred to as Ethernet or MAC address)
- ◆ Agency certifications

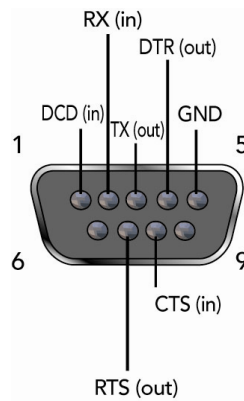
## Serial Ports

The front of the EDS4100 has four male DB9 serial ports. These ports allow you to connect up to four standard serial devices:

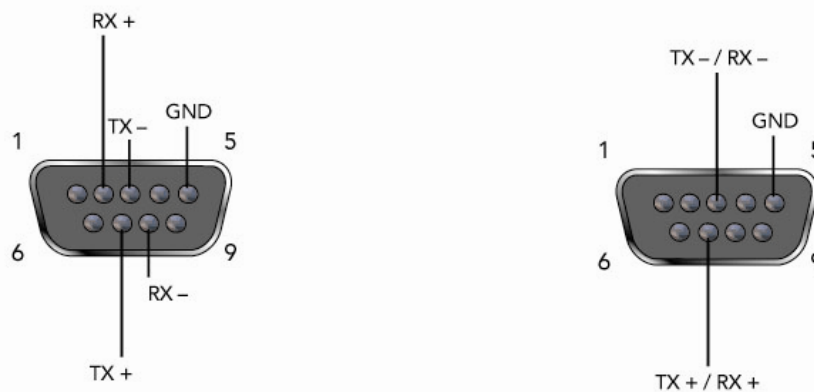
- ◆ All four serial ports support RS-232 devices. See Figure 3-3 for pin assignments.
- ◆ Serial ports 1 and 3 also support RS-422 and RS-485 serial devices. See
- ◆
- ◆ Figure 3-4 for pin assignments.

All four serial ports are configured as DTE and support baud rates up to 230,400 baud.

**Figure 3-3. RS-232 Serial Port Pins (Serial Ports 1, 2, 3, 4)**



**Figure 3-4. RS-422/RS-485 Serial Port Pins**



RS-422/485 4-wire Pin Assignments  
(Serial Ports 1 and 3)

RS-485 2-wire Pin Assignments  
(Serial Ports 1 and 3)

**Note:** Multi-drop connections are supported in 2-wire mode only.

## Ethernet Port

The back panel of the EDS4100 provides an RJ45 Ethernet port. This port can connect to an Ethernet (10 Mbps) or Fast Ethernet (100 Mbps) network. The Speed LED on the back of the EDS4100 shows the connection of the attached Ethernet network. The EDS4100 can be configured to operate at a fixed Ethernet speed and duplex mode (half- or full-duplex) or auto-negotiate the connection to the Ethernet network.

## Terminal Block Connector

The back of the EDS4100 has a terminal block screw connector for attaching to an appropriate power source, such as those used in automation and manufacturing industries. The terminal block connector supports a power range from 42 VDC to 56 VDC. It can be used with the EDS4100's barrel power connector and PoE capabilities as a redundant power source to the unit.

**Figure 3-5. Terminal Block Connector Pin Assignments**

Pin	Signal
Top	V+
Middle	V-
Bottom	Ground

## LEDs

Light-emitting diodes (LEDs) on the front and back panels show status information.

- ◆ **Back panel.** Each serial port has a Transmit and a Receive LED. The Ethernet connector has Speed and Activity LEDs. In addition, the back panel has a Power LED and a Status LED.
- ◆ **Front panel.** The front panel has a green Power LED.

The table below describes the LEDs on the back of the EDS4100.

**Figure 3-6 .Back Panel LEDs**

LED	Description
Transmit (green)	Blinking = EDS is transmitting data on the serial port.
Receive (yellow)	Blinking = EDS is receiving data on the serial port.
Power (green)	On = EDS is receiving power.
Status (yellow)	Fast blink = initial startup (loading OS). Slow blink (once per second) = operating system startup. On = unit has finished booting.
Speed (yellow)	On = EDS is connected to a 100 Mbps Fast Ethernet network. Off = EDS is connected to a 10 Mbps Ethernet network.
Activity (green)	Blink = EDS is sending data to or receiving data from the Ethernet network.

## Reset Button

The reset button is on the back of the EDS4100, to the left of the power connector. Pressing this button reboots the EDS4100 and terminates all data activity occurring on the serial and Ethernet ports.

## Physically Installing the EDS4100

### Finding a Suitable Location

- ◆ Place the EDS4100 on a flat horizontal or vertical surface. The EDS4100 comes with mounting brackets installed for vertically mounting the unit, for example, on a wall.
- ◆ If using AC power, avoid outlets controlled by a wall switch.

### Connecting the EDS4100

Observe the following guidelines when attaching serial devices:

- ◆ All four EDS4100 serial ports support RS-232 devices.
- ◆ Alternatively, ports 1 and 3 support RS-422/485 devices.
- ◆ To connect an EDS4100 serial port to another DTE device, use a null modem cable.
- ◆ To connect the EDS4100 serial port to a DCE device, use a straight-through (modem) cable.

To connect the EDS4100 to one or more serial devices, use the following procedure.

**Note:** We recommend you power off the serial devices that will be connected to the EDS4100.

1. For each serial device you want to connect, attach a serial cable between the EDS4100 and your serial device.
2. Connect an Ethernet cable between the EDS4100 Ethernet port and your Ethernet network.
3. Use one or more of the following methods to power-up the EDS4100:
  - ◆ **PoE method:** Power is supplied to the EDS4100 over the Ethernet cable by either an Ethernet switch or a midspan device.
  - ◆ **Barrel power connector:** Insert the round end of the supplied power cord into the barrel power connector on the back of the EDS4100. Plug the other end into an AC wall outlet. The barrel power connector supports a power range of 9 to 30 VDC.

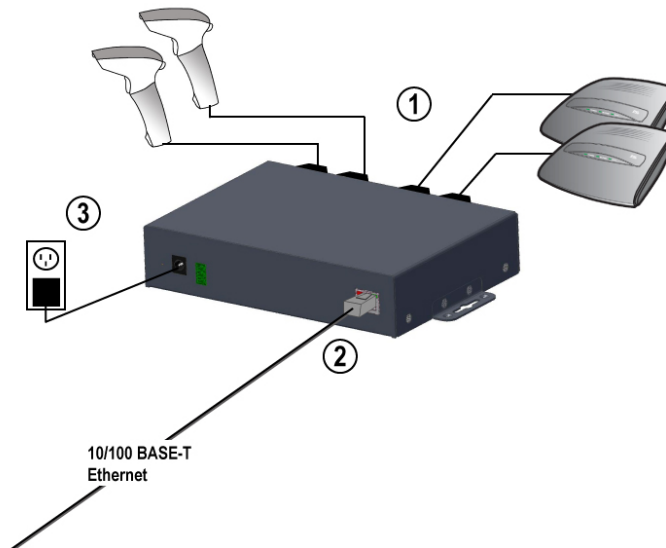
- ◆ **Terminal block connector:** Attach the power source to the terminal block connector on the back of the EDS4100. The terminal block connector supports a power range of 42 VDC to 56 VDC.

The EDS4100 powers up automatically. After power-up, the self-test begins and Evolution OS™ starts.

**Note:** These power-up methods can be used together to provide a redundant power source to the unit.

4. Power up all connected serial devices.

**Figure 3-7. Example of EDS4100 Connections**





## 4: Installation: EDS8PR, EDS16PR and EDS32PR

This chapter describes how to install the EDS8PR, EDS16PR and EDS32PR device servers.

### Package Contents

Your EDS package includes the following items:

- ◆ One EDS device server (EDS8PR, EDS16PR or EDS32PR)
- ◆ One RJ45-to-DB9Fnull modem cable
- ◆ One product CD that includes this User Guide, the Command Reference, and the Quick Start guide.
- ◆ A printed Quick Start guide

Your package may also include a power supply.

### User-Supplied Items

To complete your EDS8/16/32PR installation, you need the following items:

- ◆ RS-232 serial devices that require network connectivity. Each EDS8/16/32PR serial port supports a directly connected RS-232 serial device.
- ◆ A serial cable for each serial device to be connected to the EDS8/16/32PR. All devices attached to the device ports support the RS-232C (EIA-232) standard. Category 5 cabling with RJ45 connections is used for the device port connections.

**Note:** To connect an EDS8/16/32PR serial port to another DTE device, you need a null modem cable, such as the one supplied in your EDS8/16/32PR package. To connect the EDS8/16/32PR serial port to a DCE device, you need a straight-through (modem) cable. For a list of the Lantronix cables and adapters you can use with the EDS8/16/32PR, see [E: Lantronix Cables and Adapters](#).

- ◆ An available connection to your Ethernet network and an Ethernet cable.
- ◆ A working power outlet if the unit will be powered from an AC outlet.

## Identifying Hardware Components

Figure 3-1 shows the hardware components on the front of the EDS16PR. Figure 3-2 shows the hardware components on the back of the EDS16PR.

Figure 4-1. Front View of the EDS16PR

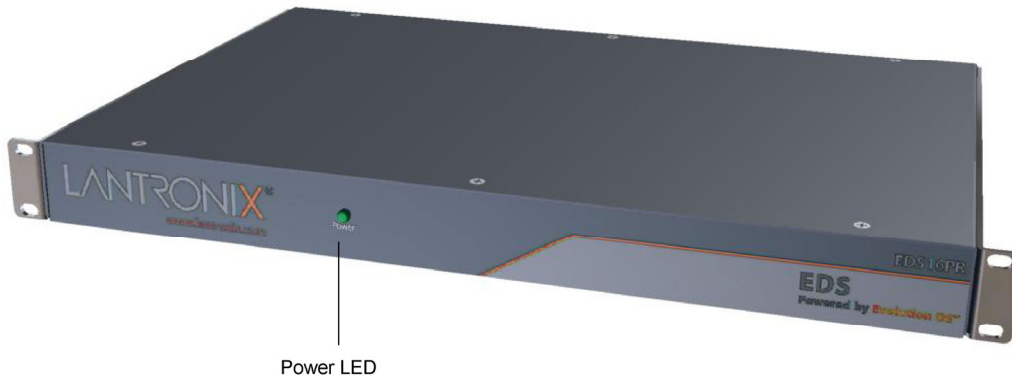
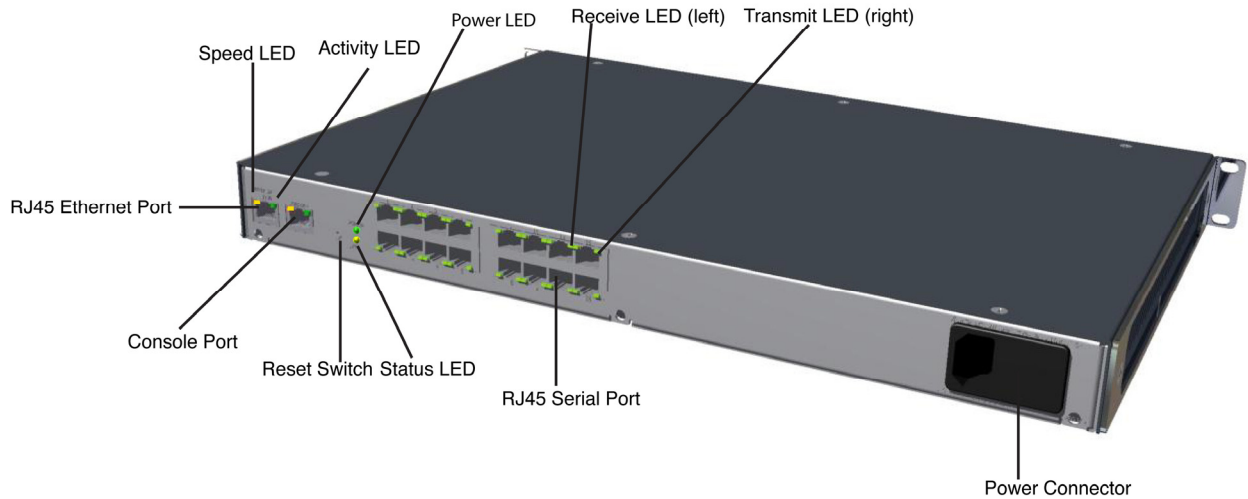


Figure 4-2. Back View of the EDS16PR



The bottom of the EDS8/16/32PR has a product information label. This label contains the following information:

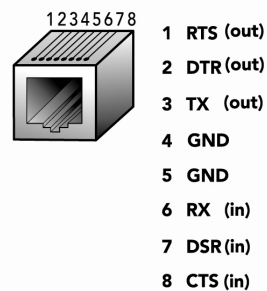
- ◆ Bar code
- ◆ Serial number

- ◆ Product ID (name)
- ◆ Product description
- ◆ Hardware address (also referred to as Ethernet or MAC address)
- ◆ Agency certifications

## Serial Ports

The EDS8PR has 8 serial ports, the EDS16PR has 16 serial ports, and the EDS32PR has 32 serial ports. All serial ports are configured as DTE and support baud rates up to 230,400 baud.

Figure 4-3. RJ45 Serial Port



## Ethernet Port

The back panel of the EDS8/16/32PR provides an RJ45 Ethernet port. This port can connect to an Ethernet (10 Mbps) or Fast Ethernet (100 Mbps) network. The Speed LED on the back of the EDS8/16/32PR shows the connection of the attached Ethernet network. The EDS8/16/32PR can be configured to operate at a fixed Ethernet speed and duplex mode (half- or full-duplex) or auto-negotiate the connection to the Ethernet network.

## LEDs

Light-emitting diodes (LEDs) on the front and back panels show status information.

- ◆ **Back panel.** Each serial port has a Transmit and a Receive LED. The Ethernet connector has a Speed and an Activity LEDs. In addition, the back panel has a Power LED and a Status LED.
- ◆ **Front panel.** The front panel has a green Power LED.

The table below describes the LEDs on the back of the EDS.

Back Panel LEDs

LED	Description
Transmit (green)	Blinking = EDS is transmitting data on the serial port.
Receive (yellow)	Blinking = EDS is receiving data on the serial port.

LED	Description
Power (green)	On = EDS is receiving power.
Status (yellow)	Fast blink = initial startup (loading OS). Slow blink (once per second) = operating system startup. On = unit has finished booting.
Speed (yellow)	On = EDS is connected to a 100 Mbps Fast Ethernet network.  Off = EDS is connected to a 10 Mbps Ethernet network.
Activity (green)	Blink = EDS is sending data to or receiving data from the Ethernet network.

## Reset Button

The reset button is on the back of the EDS8/16/32PR, to the left of the power connector. Pressing this button for 2-to-3 seconds reboots the EDS8/16/32PR and terminates all data activity occurring on the serial and Ethernet ports.

## Physically Installing the EDS8/16/32PR

### Finding a Suitable Location

- ◆ You can install the EDS8/16/32PR either in an EIA-standard 19-inch rack (1U tall) or as a desktop unit.
- ◆ If using AC power, avoid outlets controlled by a wall switch.

### Connecting the EDS8/16/32PR

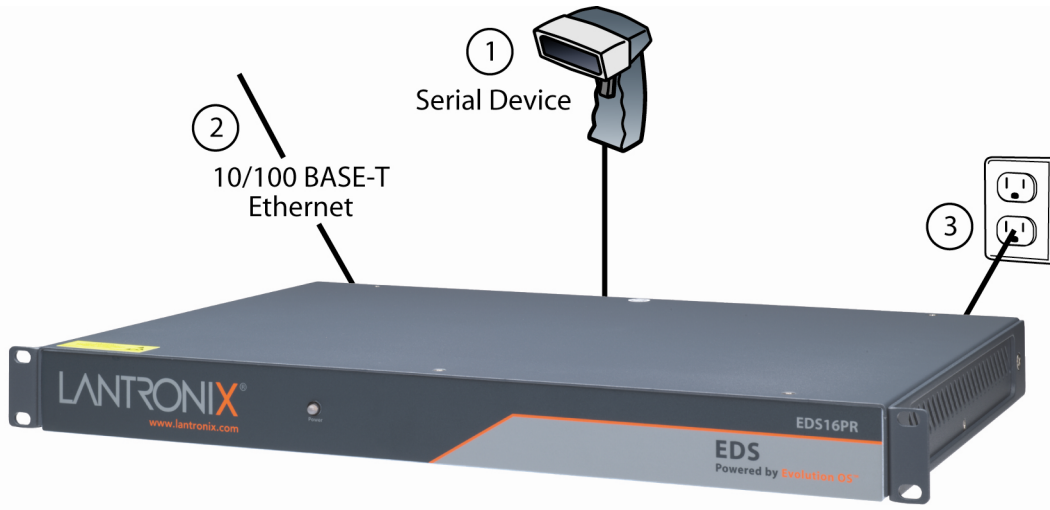
All serial ports support RS-232 devices.

To connect the EDS8/16/32PR to one or more serial devices, use the following procedure:

**Note:** We recommend you power off the serial devices that will be connected to the EDS8/16/32PR.

1. For each serial device you want to connect, attach a CAT 5 serial cable between the EDS8/16/32PR and your serial device. For a list of cables and adapters you can use with the EDS8/16/32PR, see [E: Lantronix Cables and Adapters](#).
2. Connect an Ethernet cable between the EDS8/16/32PR Ethernet port and your Ethernet network.
3. Insert the supplied power cord into the power connector on the back of the EDS8/16/32PR. Plug the other end into an AC wall outlet. After power-up, the self-test begins.
4. Power up all connected serial devices.

Figure 4-4. Example of EDS16PR Connections



## 5: Getting Started

### Using DeviceInstaller

The product CD included with your EDS package includes a program called DeviceInstaller. This program lets you view the properties of the EDS and launch EDS configuration methods.

**Note:** You can also assign an IP address and other basic network settings. For instructions, see the online Help.

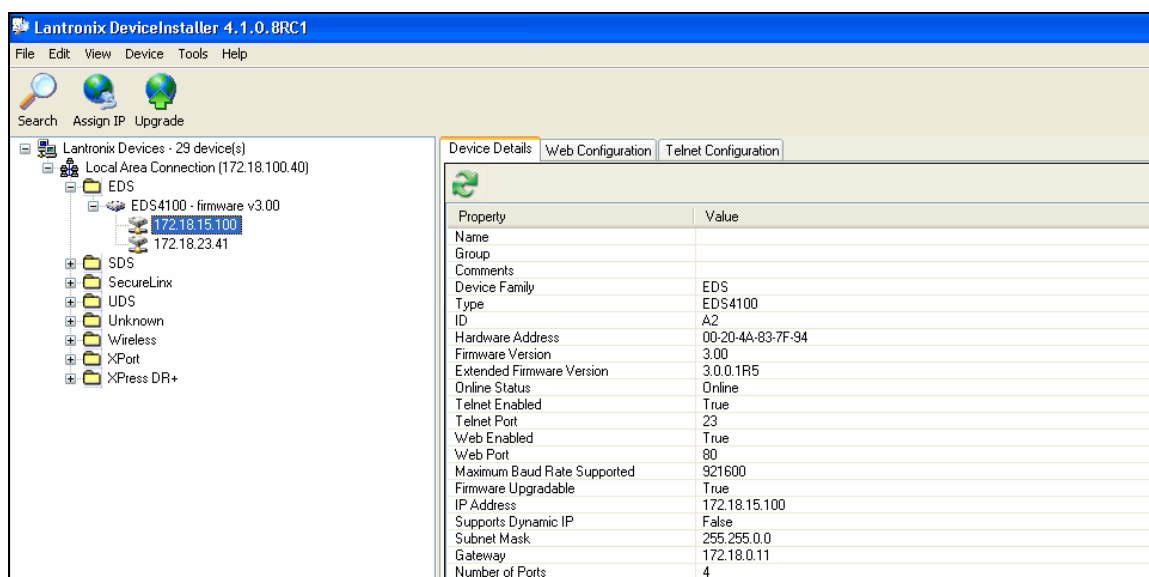
#### Starting DeviceInstaller

Follow the prompts to install DeviceInstaller.

To run DeviceInstaller:

1. From the Windows Start menu, click **Start→Programs, Lantronix→DeviceInstaller→DeviceInstaller**.
2. Click the EDS folder. The list of Lantronix EDS devices available displays.
3. Expand the list by clicking the + symbol next to the icon for the desired EDS model.
4. To view the configuration of the EDS, select the unit by clicking its IP address.

Figure 5-1. Lantronix DeviceInstaller



## Viewing EDS Properties

To view the EDS's properties, in the right window, click the **Device Details** tab. The current properties for the EDS display. Figure 5-2 lists the EDS properties and whether they are user configurable or read only. The properties of the other EDS models are similar except for the number of ports.

**Note:** On this screen, you can change **Group** and **Comments**. You can only view the remaining properties. To change them, use one of the EDS configuration methods described on page 32.

Figure 5-2. EDS4100 Properties

Property	Description
<b>Name</b>	Displays the name of the EDS, if configured.
<b>Group</b>	Enter a group to categorize the EDS. Double-click on the field, enter the value, and press <b>Enter</b> to complete.
<b>Comments</b>	Enter comments for the EDS. Double-click on the field, type in the value, and press <b>Enter</b> to complete.
<b>Device Family</b>	Displays the EDS's device family type as <b>EDS</b> .
<b>Type</b>	Displays the device type as <b>EDS</b> .
<b>ID</b>	Displays the EDS's ID embedded within the box.
<b>Hardware Address</b>	Displays the EDS's hardware address.
<b>Firmware Version</b>	Displays the firmware currently installed on the EDS.
<b>Extended Version</b>	Displays the full version of firmware currently installed on the UDS.
<b>Online Status</b>	Displays the EDS status. Online = the EDS is online. Offline = the EDS is offline. Unreachable = the EDS is on a different subnet. Busy = the EDS is currently performing a task.
<b>Telnet Enabled</b>	Displays whether Telnet is enabled on this EDS.
<b>Telnet Port</b>	Displays the EDS's port for Telnet sessions.
<b>Web Enabled</b>	Displays whether Web Manager access is enabled on this EDS.
<b>Web Port</b>	Displays the EDS's port for Web Manager configuration.
<b>Maximum Baud Rate Supported</b>	Displays the EDS's maximum baud rate. <b>Note:</b> The EDS may not be operating at this rate.
<b>Firmware Upgradeable</b>	Displays <b>True</b> if the EDS firmware is upgradeable.
<b>IP Address</b>	Displays the EDS's current IP address. To change it, click the <b>Assign IP</b> button on the DeviceInstaller menu bar.

Property	Description
<b>Supports Dynamic IP</b>	Displays <b>True</b> if the EDS automatically receives an IP address (e.g., from DHCP). Displays <b>False</b> if not.
<b>Subnet Mask</b>	Displays the subnet mask specifying the network segment on which the EDS resides.
<b>Gateway</b>	Displays the IP address of the router of this network. There is no default.
<b>Number of Ports</b>	Displays the number of ports on this EDS.

**Note:** These parameters are stored on the computer running DeviceInstaller.

## Configuration Methods

When your EDS boots for the first time, it automatically loads its factory-default configuration settings. For a list of the factory-default configuration settings, see [A: Factory Default Configuration](#).

For convenience, there are three ways to configure the EDS.

- ◆ Using the Web Manager interface
- ◆ Using the CLI through a SSH/Telnet session or an EDS8/16/32PR serial port.
- ◆ Using the XML interface

These unified configuration methods provide access to all features, giving you the same level of control over the EDS8/16/32PR regardless of the configuration method you choose.

### Configuring from the Web Manager Interface

With this method, you can use a Web browser to configure the EDS using a Web-based graphical point-and-click interface. The advantages to this method are ease of use and location independence. With this method, you can configure the EDS from any location that has access to a Web browser and the Internet.

### Configuring via an SSH/Telnet Session or Serial Port Using the CLI

The EDS provides a command-line interface (CLI) designed to enable the configuration and systems management functions that can also be performed through the Web Manager and XML interfaces. To configure the EDS using the CLI, you must either start an SSH or Telnet session or use a terminal or a computer attached to one of the EDS serial ports or the console port on the EDS8/16/32PR.

The difference between the SSH/Telnet and serial interfaces is the physical connection paths to the EDS. With an SSH/Telnet session, you can configure the unit without having to be in the same location as the EDS. The serial-interface method, however, requires a terminal or computer to be attached to an available EDS serial port. This means the terminal or computer must be in the same location as the EDS.

For more information, see the **EDS Command Reference** on the product CD or the Lantronix web site ([www.lantronix.com](http://www.lantronix.com)).



## Configuring from the XML Interface

The EDS also provides an XML interface that can be used to perform configuration and systems-management functions. This configuration method lets you automate the configuration process using XML configuration files. This method is particularly convenient if you have multiple EDS device servers that will use the same configuration settings, because you can define a configuration profile that can be imported by, and shared among, your other EDS device servers.

For more information, see the **EDS Command Reference** on the product CD or the Lantronix web site ([www.lantronix.com](http://www.lantronix.com)).

## 6: Configuration Using the Web Manager

This chapter describes how to configure the EDS using the Web Manager, Lantronix's browser-based configuration tool. The unit's configuration is stored in nonvolatile memory and retained without power. All changes take effect immediately, unless otherwise noted.

### Accessing the Web Manager through a Web Browser

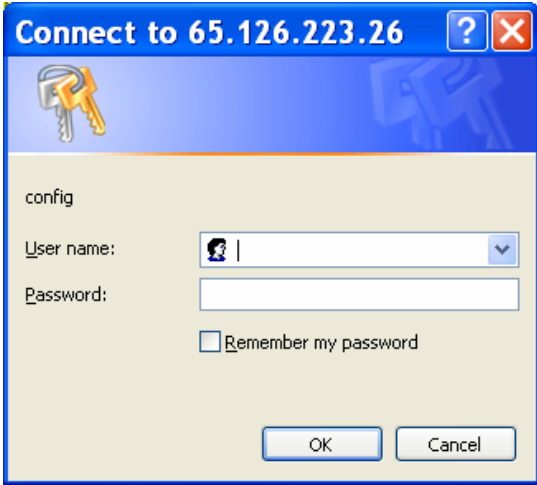
The following procedure describes how to log into the EDS using a standard Web browser.

**Note:** Alternatively, access the Web Manager by selecting the **Web Configuration** tab from DeviceInstaller (see [Viewing EDS Properties on page 31](#)).

To access Web Manager:

1. Open a standard Web browser such as Netscape Navigator 6.x and later, Internet Explorer 5.5. and later, Mozilla Suite, Mozilla Firefox, or Opera.
2. Enter the IP address of the EDS in the address bar. The EDS's built-in security requires you to log in with your user name and password-

Figure 6-1. Prompt for User Name and Password



The screenshot shows a standard Windows-style dialog box. The title bar reads "Connect to 65.126.223.26" with a question mark icon and a close button. Below the title bar is a blue header area with a key icon. The main content area is light gray and contains the text "config" at the top. Below that are two labels: "User name:" followed by a dropdown menu, and "Password:" followed by a text input field. A checkbox labeled "Remember my password" is positioned below the password field. At the bottom of the dialog are two buttons: "OK" and "Cancel".

3. Enter your user name and password in the appropriate fields. The Device Status page displays (see Figure 6-2). This page is the Web Manager home page.

**Note:** The factory-default user name is **admin** and the factory-default password is **PASS**. After you log in to the Web Manager, we recommend you use the FTP page to change the default FTP password (see page 72), the HTTP Authentication Page to change the HTTP authentication password (see page 79), and the Command Line Interface Configuration Page to change the CLI password (see page 115).

Figure 6-2. Web Manager Device Status Page

The screenshot displays the 'Device Status' page for a Lantronix EDS4100 device. The page features a navigation menu on the left with options like Status, Network, Line, Tunnel, DNS, SNMP, FTP, TFTP, Syslog, HTTP, CLI, Email, SSH, SSL, XML, Filesystem, Protocol Stack, IP Address Filter, Query Port, Diagnostics, and System. The main content area is titled 'Device Status' and contains the following information:

Product Information		
Product Type:	Lantronix EDS4100	
Firmware Version:	3.0.0.1R1	
Build Date:	Jul 27 2006 (15:24:24)	
Serial Number:	05062027554PLG	
Uptime:	5 days 19:21:15	
Permanent Config:	Saved	
Network Settings		
Ethernet:	Auto (100Mbps Full)	
MAC Address:	00:20:4a:83:7f:94	
Host:		
IP Address:	172.18.15.100 / 255.255.0.0	
Default Gateway:	172.18.0.1	
Domain:	support.int.lantronix.com	
Primary DNS:	172.18.0.11	
Secondary DNS:	172.16.1.26	
Line Settings		
Line 1:	RS232, 9600, N, 8, 1, None	
Line 2:	RS232, 9600, N, 8, 1, None	
Line 3:	RS232, 9600, N, 8, 1, None	
Line 4:	RS232, 9600, N, 8, 1, None	
Tunneling		
	Connect Mode	Accept Mode
Tunnel 1:	Disabled	Waiting
Tunnel 2:	Disabled	Waiting
Tunnel 3:	Disabled	Waiting
Tunnel 4:	Disabled	Waiting

Copyright © Lantronix, Inc. 2005. All rights reserved.

## Navigating Through the Web Manager

The Web Manager provides an intuitive point-and-click interface. A menu bar at the left side of each page provides links you can click to navigate from one page to another. Some pages are read-only, while others let you change configuration settings.

**Note:** *There may be times when you must reboot the EDS for the new configuration settings to take effect. The chapters that follow indicate when a change requires a reboot.*

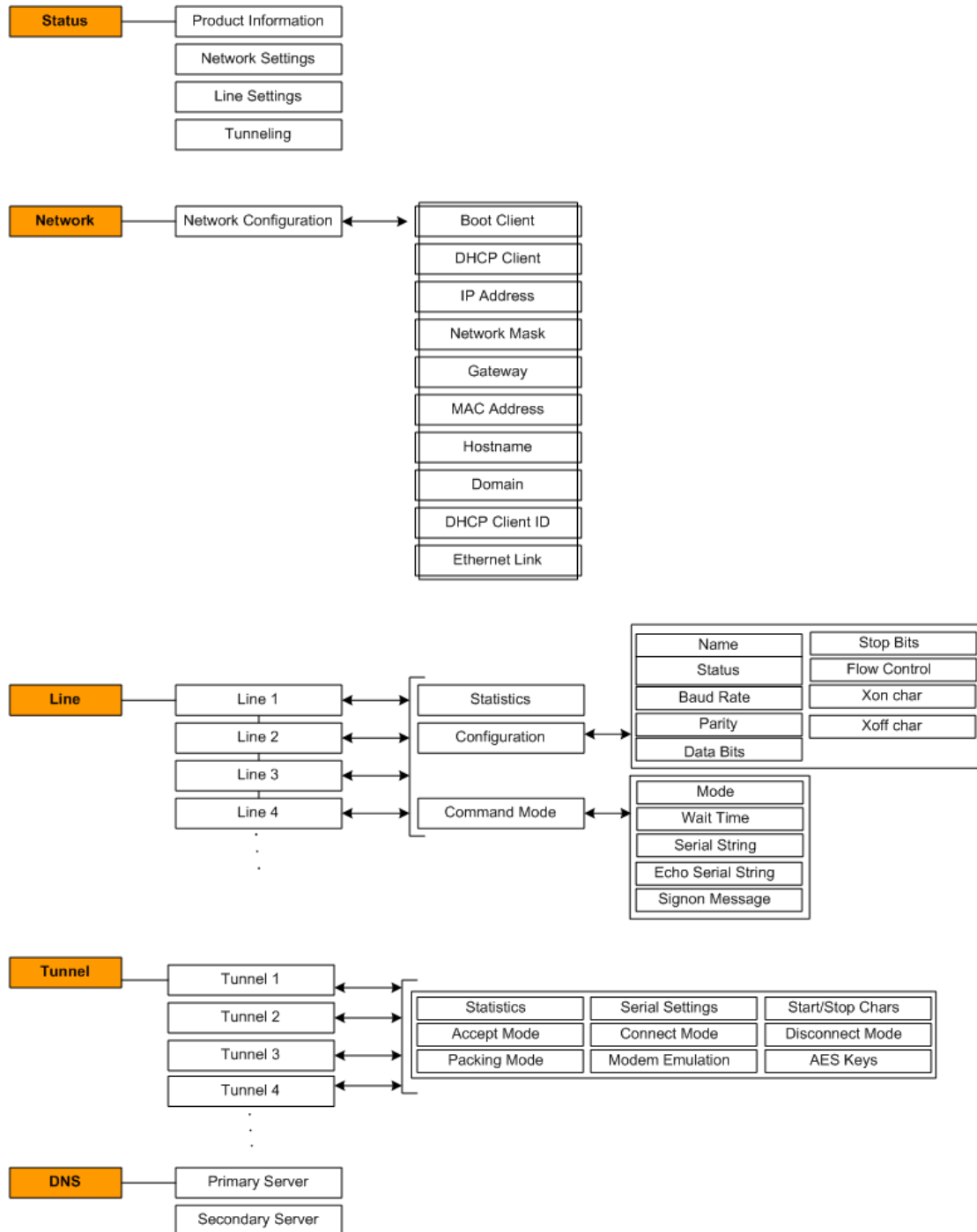
Figure 6-6 shows the structure of the multilevel Web Manager configuration pages.

Summary of Web Manager Pages

Page	Description	See Page
Device Status	Displays EDS product information and network, line, and tunneling settings.	40
Network	Lets you configure the current network interface on the EDS.	44
Line	Displays statistics and lets you change the current configuration and Command mode settings of 4 serial lines for the EDS4100, 16 serial lines for the EDS16PR, and 32 serial lines for the EDS32PR.	47
Tunnel	Displays the current connection statistics and lets you change the current configuration settings for up to 4 tunnels for the EDS4100, 16 tunnels for the EDS16PR, and 32 tunnels for the EDS32PR.	52
DNS	Displays the current configuration of the DNS subsystem and lets you change primary and secondary DNS servers.	70
SNMP	Displays and lets you change the current Simple Network Management Protocol (SNMP) configuration settings.	71
FTP	Displays statistics and lets you change the current configuration for the File Transfer Protocol (FTP) server.	72
TFTP	Displays statistics and lets you change the current configuration for the Trivial File Transfer Protocol (TFTP) server.	74
Syslog	Lets you specify the severity of events to log and the server and ports to which the syslog should be sent.	75
HTTP	Displays HyperText Transfer Protocol (HTTP) statistics and lets you change the current configuration, authentication, and RSS settings.	75
CLI	Displays Command Line Interface (CLI) statistics and lets you change the current CLI configuration settings.	84
Email	Displays email statistics and lets you clear the email log, configure email settings, and send an email.	111
SSH	Displays and lets you change the configuration settings for SSH server host keys, SSH server authorized users, SSH client known hosts, and SSH client users.	111
SSL	Lets you upload an existing certificate or create a new self-signed certificate.	92
XML	Lets you export XML configuration and status records, and import	117

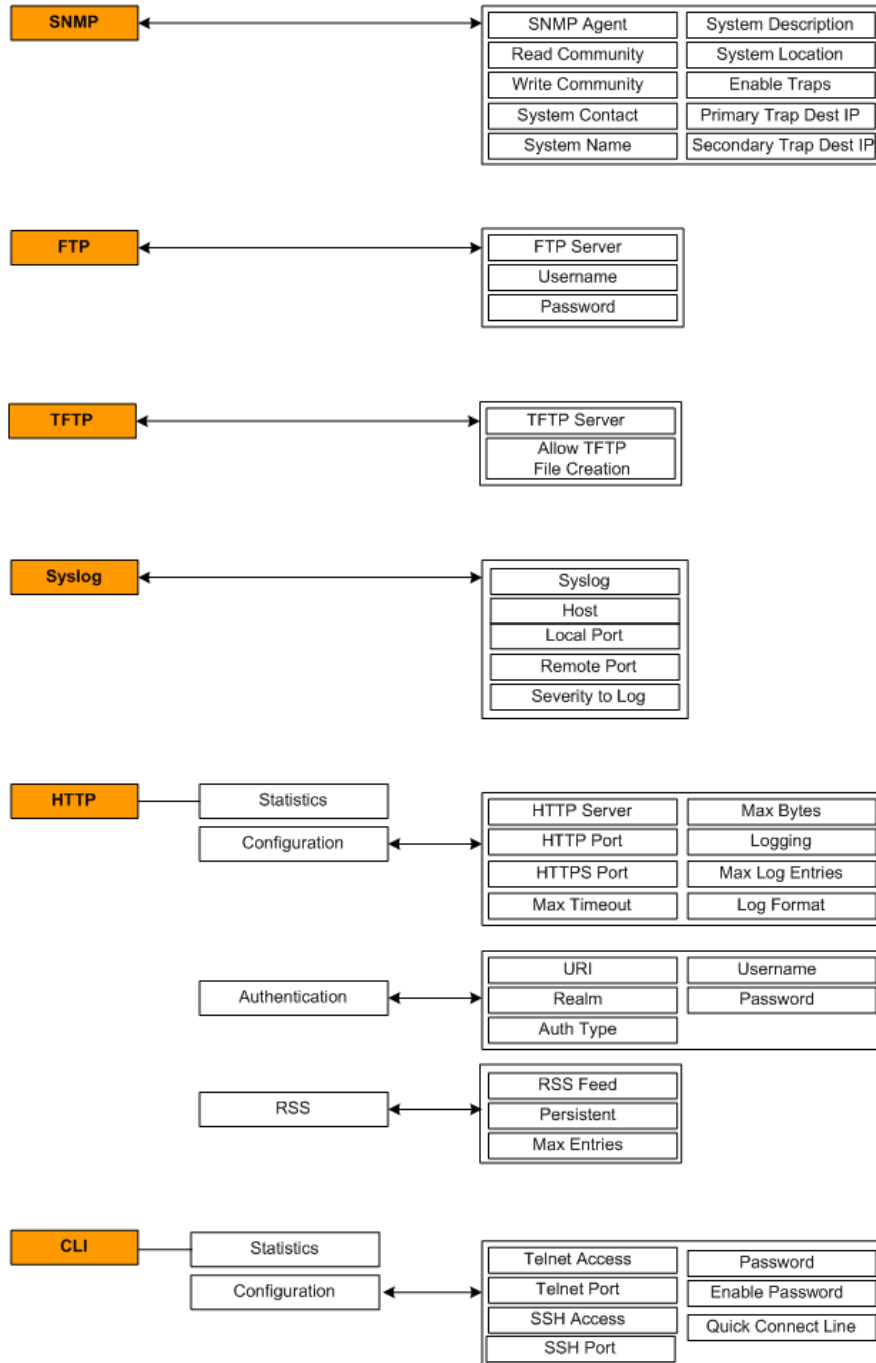
Page	Description	See Page
	XML configuration records.	
Filesystem	Displays filesystem statistics and lets you browse the filesystem to create a file or directory, upload files using HTTP, copy a file, move a file, or perform TFTP actions.	95
Protocol Stack	Lets you perform lower level network stack-specific activities.	122
IP Address Filter	Lets you specify all the IP addresses and subnets that are allowed to send data to this device.	124
Query Port	Displays and lets you change configuration settings for the query port.	109
Diagnostics	Lets you perform various diagnostic procedures.	95
System	Lets you reboot the EDS, restore factory defaults, upload new firmware, change the EDS's long and short names, and change the time setting.	107

Figure 6-3. Web Manager Menu Structure (1 of 4)



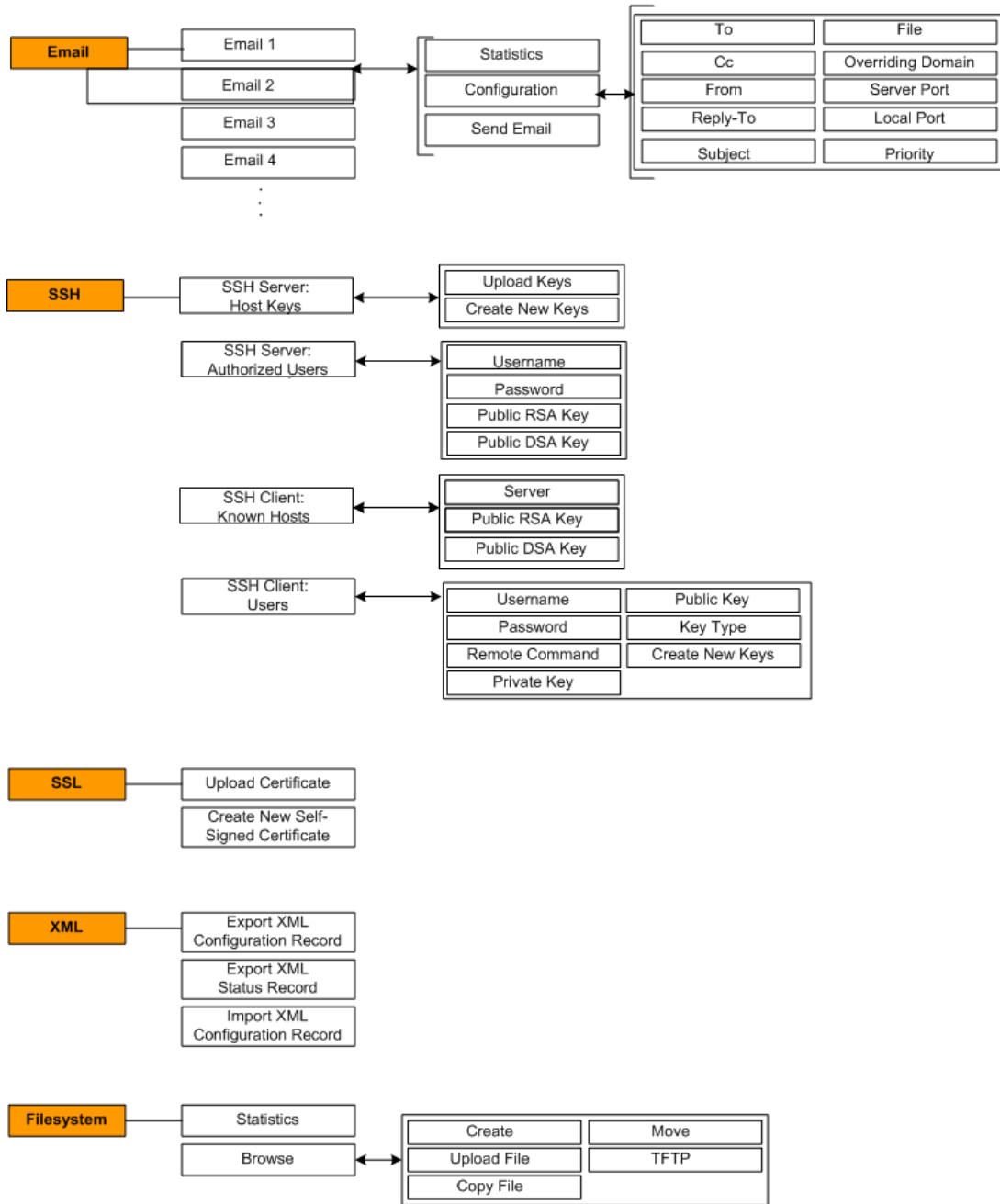
(continued on next page)

Figure 6-4. Web Manager Menu Structure (2 of 4)



(continued on next page)

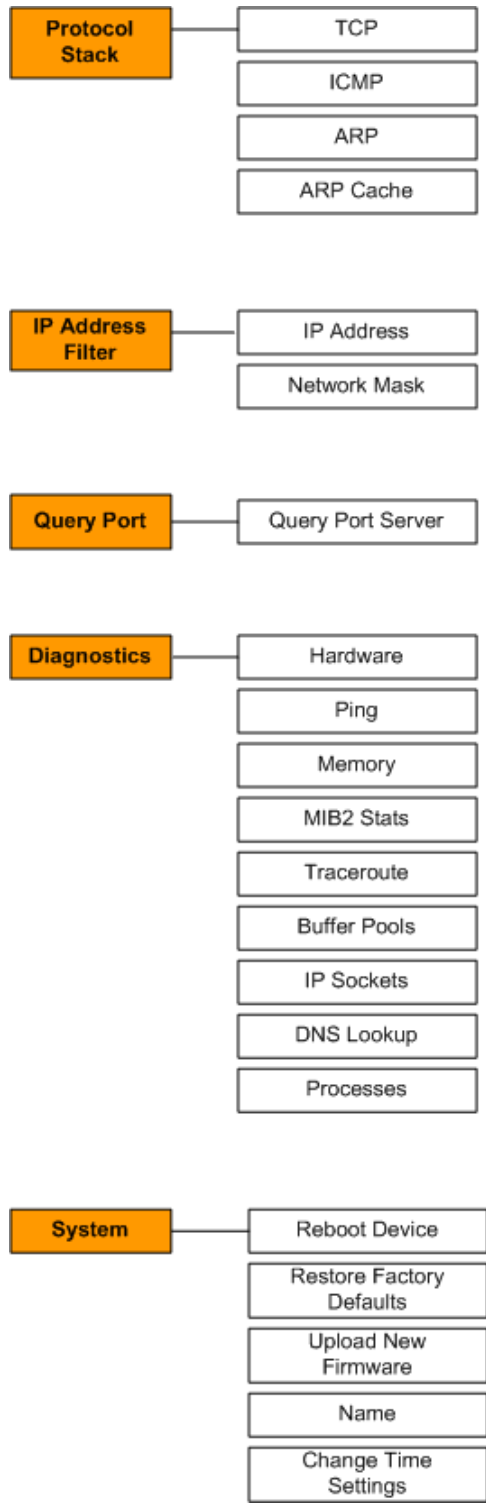
Figure 6-5. Web Manager Menu Structure (3 of 4)



(continued on next page)

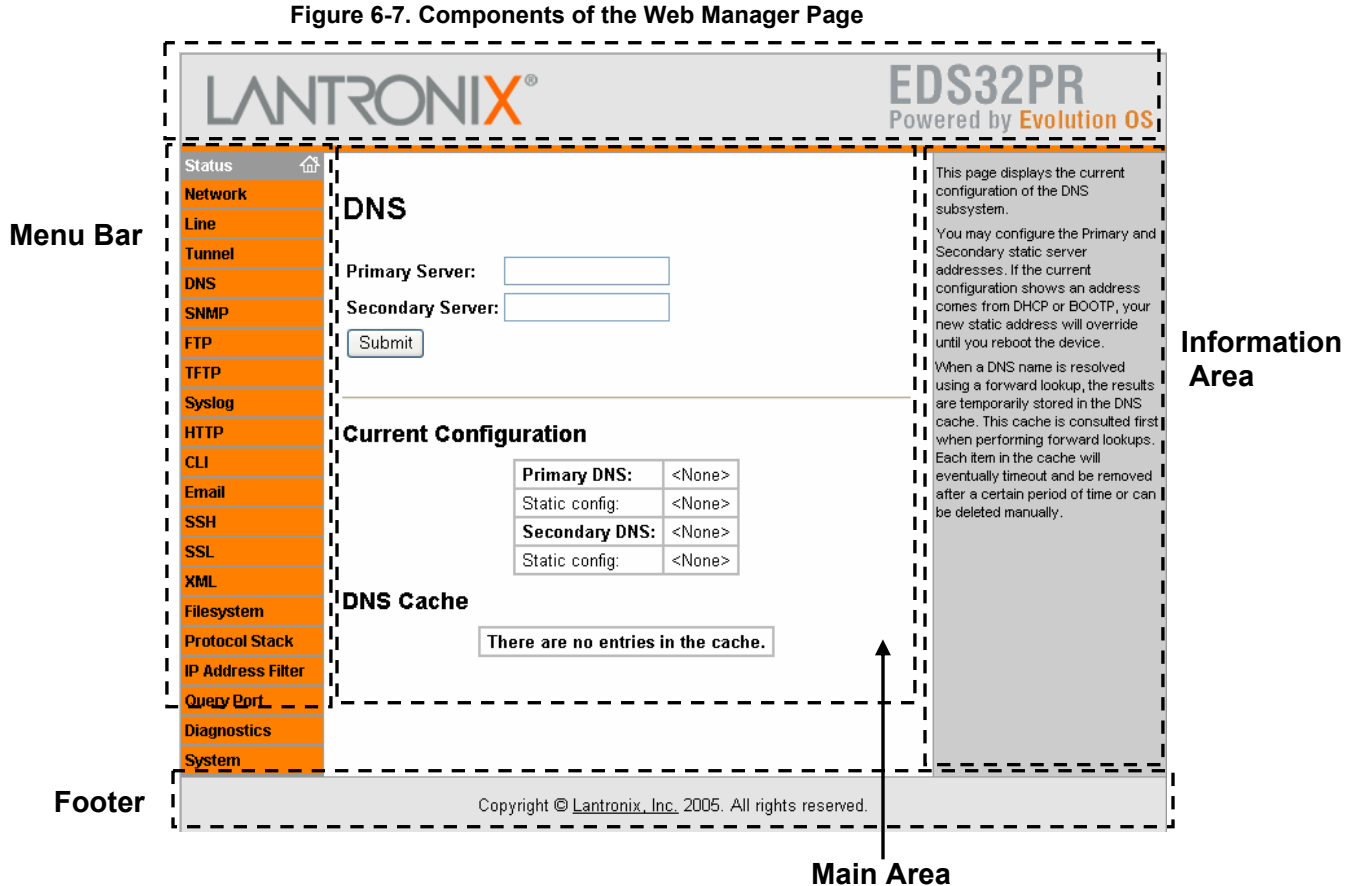


Figure 6-6. Web Manager Menu Structure (4 of 4)



## Understanding the Web Manager Pages

Figure 6-7 shows the areas of the Web Manager page.



The header always displays at the top of the page. The header information remains the same regardless of the page displayed.

The menu bar always displays at the left side of the page, regardless of the page displayed. The menu bar lists the names of the pages available in the Web Manager. To display a page, click it in the menu bar.

When you click the name of a page in the menu bar, the page displays in the main area. The main area of most pages is divided into two sections:

- ◆ The top section lets you select or enter new configuration settings. After you change settings, click the **Submit** button to apply the change. Some settings require the EDS to be rebooted before the settings take effect. Those settings are identified in the appropriate sections in this chapter.
- ◆ The bottom section shows the current configuration.


The information area shows information or instructions associated with the page.

The footer displays at the bottom of the page. It contains copyright information and a link to the Lantronix home page.

## Device Status Page

The Device Status page is the first page that displays when you log into the Web Manager. It also displays when you click the **Status** link in the menu bar. This read-only page shows the EDS product information, network settings, line settings, and tunneling settings.

Figure 6-8. Device Status Page (EDS4100)



**EDS4100**  
 Powered by Evolution OS

- Status
- Network
- Line
- Tunnel
- DNS
- SNMP
- FTP
- TFTP
- Syslog
- HTTP
- CLI
- Email
- SSH
- SSL
- XML
- Filesystem
- Protocol Stack
- IP Address Filter
- Query Port
- Diagnostics
- System

### Device Status

Product Information		
Product Type:	Lantronix EDS4100	
Firmware Version:	3.0.0.1R1	
Build Date:	Jul 27 2006 (15:24:24)	
Serial Number:	05062027554PLG	
Uptime:	5 days 19:21:15	
Permanent Config:	Saved	
Network Settings		
Ethernet:	Auto (100Mbps Full)	
MAC Address:	00:20:4a:83:7f:94	
Host:		
IP Address:	172.18.15.100 / 255.255.0.0	
Default Gateway:	172.18.0.1	
Domain:	support.int.lantronix.com	
Primary DNS:	172.18.0.11	
Secondary DNS:	172.16.1.26	
Line Settings		
Line 1:	RS232, 9600, N, 8, 1, None	
Line 2:	RS232, 9600, N, 8, 1, None	
Line 3:	RS232, 9600, N, 8, 1, None	
Line 4:	RS232, 9600, N, 8, 1, None	
Tunneling	Connect Mode	Accept Mode
Tunnel 1:	Disabled	Waiting
Tunnel 2:	Disabled	Waiting
Tunnel 3:	Disabled	Waiting
Tunnel 4:	Disabled	Waiting

Copyright © Lantronix, Inc. 2005. All rights reserved.

## 7: Network, Serial Line, and Tunnel Settings

### Network Configuration Page

Clicking the **Network** link in the menu bar displays the Network Configuration page. Here you can change the following EDS network configuration settings:

- ◆ BOOTP and DHCP client
- ◆ IP address, network mask, and gateway
- ◆ MAC address
- ◆ Hostname and domain
- ◆ DHCP client ID
- ◆ Ethernet transmission speed

Figure 7-1. Network Configuration

LANTRONIX®
EDS4100  
Powered by Evolution OS

Status

**Network**

Line

Tunnel

DNS

SNMP

FTP

TFTP

Syslog

HTTP

CLI

Email

SSH

SSL

XML

Filesystem

Protocol Stack

IP Address Filter

Query Port

Diagnostics

System

### Network Configuration

BOOTP Client:  On  Off  
 DHCP Client:  On  Off  
 IP Address:   
 Network Mask:   
 Gateway:   
 MAC Address:   
 Hostname:   
 Domain:   
 DHCP Client ID:   
 Ethernet Link: Speed:  Auto  10Mbps  100Mbps  
 Duplex:  Auto  Half  Full

---

#### Current Configuration

	Current	After Reboot
BOOTP Client:	Off	Off
DHCP Client:	Off	Off
IP Address:	172.18.15.100 <a href="#">[Delete]</a>	172.18.15.100 <a href="#">[Delete]</a>
Network Mask:	255.255.0.0 <a href="#">[Delete]</a>	255.255.0.0 <a href="#">[Delete]</a>
Gateway:	172.18.0.11 <a href="#">[Delete]</a>	172.18.0.11 <a href="#">[Delete]</a>
MAC Address:	00:20:4a:83:7f:94	00:20:4a:83:7f:94
Hostname:	<None>	<None>
Domain:	int.lantronix.com <a href="#">[Delete]</a>	int.lantronix.com <a href="#">[Delete]</a>
DHCP Client ID:	<None>	<None>
Ethernet:	Auto 10/100 Mbps Auto Half/Full (100 Mbps Full)	Auto 10/100 Mbps Auto Half/Full

This page is used to configure the Network interface on the device.

There are two configuration tables displayed. The first table shows the current running configuration. The second table shows the configuration that will take effect after the device is rebooted.

The following items require a reboot to take effect:

- BOOTP On/Off
- DHCP On/Off
- IP Address
- Network Mask
- MAC Address
- DHCP Client ID

If there is an IP Address, Network Mask, Gateway, Hostname, or Domain configured for the device and BOOTP or DHCP is turned on, the original configuration items are ignored. BOOTP/DHCP will auto-discover and eclipse those configuration items.

If both BOOTP and DHCP are turned on, DHCP has higher precedence and BOOTP will not get executed.

When BOOTP or DHCP fails to discover an IP Address, a new address will automatically be generated using AutoIP. This address will be within the 169.254.x.x space.

Copyright © Lantronix, Inc. 2005. All rights reserved.

The bottom part of this page shows the current configuration. The **After Reboot** column in the **Current Configuration** section of this page shows the settings that will take effect the next time the EDS reboots.

Changes to the following settings require the EDS to be rebooted before the new settings take effect:

- ◆ **BOOTP Client**
- ◆ **DHCP Client**
- ◆ **IP Address**
- ◆ **Network Mask**
- ◆ **MAC Address**
- ◆ **DHCP Client ID**

**Notes:** Some settings in the **Current Configuration** section, such as **IP Address** and **Network Mask** have a **Delete** link you can click to delete the setting. If you click this link, a warning message asks whether you are sure you want to delete the setting. Click **OK** to delete the setting or **Cancel** to keep it.

#### Network Configuration Page Settings

Network Configuration Page Settings	Description
BOOTP Client	<p>Select whether the EDS should send BOOTP requests. Changing this value requires the EDS to be rebooted. Choices are:</p> <p><b>On</b> = EDS sends BOOTP requests on a DHCP-managed network. This setting overrides the configured IP address, network mask, gateway, host name, and domain settings. If DHCP is set to On, the EDS automatically uses DHCP, regardless of whether BOOTP Client is set to On.</p> <p><b>Off</b> = EDS does not send BOOTP requests.</p>
DHCP Client	<p>Select whether the EDS IP address is automatically assigned by a DHCP server. Changing this value requires the EDS to be rebooted. Choices are:</p> <p><b>On</b> = EDS receives its IP address automatically from a DHCP server, regardless of the BOOTP Client setting. This setting overrides the configured IP address, network mask, gateway, host name, and domain settings.</p> <p><b>Off</b> = EDS does not receive its IP address automatically.</p>
IP Address	<p>Enter the EDS static IP address. The IP address consists of four octets separated by a period and is used if BOOTP and DHCP are both set to Off. Changing this value requires the EDS to be rebooted.</p> <p><b>Note:</b> When DHCP is enabled, the EDS tries to obtain an IP address from DHCP. If it cannot, the EDS uses an Auto IP address in the range of 169.254.xxx.xxx.</p>

Network Configuration Page Settings	Description
Network Mask	Enter the EDS subnet mask. The subnet mask consists of four octets separated by a period. Changing this value requires the EDS to be rebooted.  <i>Note: When DHCP is enabled, the EDS tries to obtain a network mask from DHCP. If it cannot, the EDS uses a network mask of 255.255.0.0.</i>
Gateway	Enter the router IP address from the local LAN the EDS is on. The address consists of four octets separated by a period.
MAC Address	Enter the EDS MAC address. Default is factory set. Changing this value may cause unexpected results. Changing this value requires the EDS to be rebooted.
Hostname	Enter the EDS host name. The host name can be up to 31 characters with no spaces.
Domain	Enter the EDS domain name.
DHCP Client ID	Enter a DHCP ID if used by the DHCP server. Changing this value requires the EDS to be rebooted.
Ethernet Link	Select the Ethernet link speed. Default is Auto.

## Line Settings Pages

The Line Settings page displays the status and statistics for each of the serial lines (ports). This page also lets you change the character format and command mode settings for the serial lines.

To select a line:

**EDS4100:** Click **Line 1**, **Line 2**, **Line 3**, or **Line 4** at the top of the page.

**EDS8/16/32PR:** Select the line from the **Select Line** drop-down list at the top of the page.

After you select a serial line, you can click **Statistics**, **Configuration**, or **Command Mode** to view and change the settings of the selected serial line. Because all serial lines operate independently, you can specify different configuration settings for each line.

## Line – Statistics Page

The Line – Statistics page displays when you click **Line** in the menu bar. It also displays when you click **Statistics** at the top of one of the other Line Settings pages. This read-only page shows the status and statistics for the serial line selected at the top of this page.

Figure 7-2. Line –Statistics Page

The screenshot shows the LANTRONIX EDS32PR web interface. The top header includes the LANTRONIX logo and 'EDS32PR Powered by Evolution OS'. A left-hand navigation menu lists various settings categories. The main content area is titled 'Line 1- Statistics' and features a table of statistics for the selected line. A 'Select Line' dropdown menu is set to 'Line 1', and there are buttons for 'Statistics', 'Configuration', and 'Command Mode'. A right-hand sidebar contains a note: 'This page displays the current status and various statistics for the Serial Line.' The footer of the page contains the copyright notice: 'Copyright © Lantronix, Inc., 2005. All rights reserved.'

	Receiver	Transmitter
Bytes:	18897	2322251
Breaks:	0	0
Flow control:	N/A	N/A
Parity Errors:	0	
Framing Errors:	0	
Overrun Errors:	0	
No Rx Buffer Errors:	0	
Queued Receive Bytes:	0	
Queued Transmit Bytes:	0	
CTS input:	not asserted	
RTS output:	asserted	
DSR input:	not asserted	
DTR output:	not asserted	



## Line - Configuration Page

If you click **Configuration** at the top of one of the Line Settings pages, the Line – Configuration page displays. This page shows the configuration settings for the serial line selected at the top of the page and lets you change the settings for that serial line.

Figure 7-3. Configuration Page

**LANTRONIX®** EDS32PR  
Powered by Evolution OS

Status Network Line Tunnel DNS SNMP FTP TFTP Syslog HTTP CLI Email SSH SSL XML Filesystem Protocol Stack IP Address Filter Query Port Diagnostics System

Select Line: Line 1

Statistics Configuration Command Mode

### Line 1- Configuration

	Current Setting	Change Setting To
Name:		<input type="text"/>
Status:	Enabled	Enabled <input type="button" value="v"/>
Baud Rate:	9600	9600 <input type="button" value="v"/> Custom <input type="text"/>
Parity:	None	None <input type="button" value="v"/>
Data Bits:	8	8 <input type="button" value="v"/>
Stop Bits:	1	1 <input type="button" value="v"/>
Flow Control:	None	None <input type="button" value="v"/>
Xon char:	0x11 ( \17 )	<input type="text"/>
Xoff char:	0x13 ( \19 )	<input type="text"/>
		<input type="button" value="Submit"/>

This page displays the current configuration of the Serial Line. Changing any of the fields takes effect immediately.

When specifying a **Custom** baud rate, select 'Custom' from the drop down list and then enter the desired rate in the text box.

When specifying either **Xon char** or **Xoff char**, either prefix decimal with \ or prefix hexadecimal with 0x or provide a single printable character. These are used when **Flow Control** is set to Software. The default Xon char is 0x11. The default Xoff char is 0x13.

Copyright © Lantronix, Inc. 2005. All rights reserved.

### Configuration Page

Line – Configuration Page Settings	Description
Name (optional)	Enter a name for the serial port. The name may have up to 25 characters.
Status	Select to enable or disable the selected EDS serial port.
Baud Rate	Select the baud rate for the currently selected serial port. Choices are:  <b>300</b> baud to <b>230,400</b> baud. Default is 9600 baud.  <b>Custom</b> = lets you enter in the <b>Custom</b> text box a speed other than those shown.

Line – Configuration Page Settings	Description
Parity	Select the parity used by the currently selected serial line. Choices are:  <b>None (default)</b>  <b>Even</b>  <b>Odd</b>
Data Bits	Select the number of data bits used by the currently selected serial line. Choices are:  <b>7</b>  <b>8 (default)</b>
Stop Bits	Select the number of stop bits used by the currently selected serial line. Choices are:  <b>1 (default)</b>  <b>2</b>
Flow Control	Select the flow control method used by the currently selected serial line. Choices are:  <b>None (default)</b>  <b>Hardware</b>  <b>Software</b>
Xon char	Character to use to initiate a flow of data.  When <b>Flow Control</b> is set to <b>Software</b> , specify <b>Xon char</b> . Prefix a decimal character with \ or a hexadecimal character with 0x, or provide a single printable character. The default Xon char is 0x11.
Xoff char	When <b>Flow Control</b> is set to <b>Software</b> , specify <b>Xoff char</b> . Prefix a decimal character with \ or a hexadecimal character with 0x, or provide a single printable character. The default Xoff char is 0x13.

## Line – Command Mode Page

If you click **Command Mode** at the top of one of the Line Settings pages, the Line – Command Mode page displays. This page shows the command mode settings for the serial line selected at the top of the page and lets you change the settings for that serial line.

Figure 7-4. Line – Command Mode Page

The screenshot shows the LANTRONIX EDS4100 web interface. The top navigation bar includes tabs for Line 1, Line 2, Line 3, and Line 4. The 'Command Mode' tab is selected. The main configuration area is titled 'Line 1- Command Mode' and contains the following settings:

- Mode:** Radio buttons for Always, Use Serial String, and Disabled.
- Wait Time:** A text input field followed by 'milliseconds'.
- Serial String:** A text input field with radio buttons for Text (selected) and Binary.
- Echo Serial String:** Radio buttons for Yes and No.
- Signon Message:** A text input field with radio buttons for Text (selected) and Binary.
- A **Submit** button.

Below the configuration fields is a 'Current Configuration' table:

<b>Mode:</b>	Disabled (Inactive)
<b>Wait Time:</b>	5000milliseconds
<b>Serial String:</b>	<None>
<b>Echo Serial String:</b>	On
<b>Signon Message:</b>	<None>

On the right side of the page, there is explanatory text:

When Command Mode is enabled, the Command Line Interface (CLI) is attached to the Serial Line. Command Mode can be enabled in a number of ways:

- The **Always** choice immediately enables Command Mode for the Serial Line.
- The **Use Serial String** choice enables Command Mode when the Serial String is read on the Serial Line during boot time.
- The **Wait Time** specifies the amount of time to wait during boot time for the Serial String. This timer starts right after the Signon Message has been sent on the Serial Line.
- The **Serial String** is a string of bytes that must be read on the Serial Line during boot time in order to enable Command Mode. It may contain a **time element** to specify a required delay in milliseconds *x*, formed as {*x*}.
- The **Signon Message** is a string of bytes that is sent on the Serial Line during boot time.
- Binary** form is a string of characters representing byte values where each Hexadecimal byte value starts with \0x and each Decimal byte value starts with \.

At the bottom of the page, the copyright notice reads: Copyright © Lantronix, Inc., 2005. All rights reserved.

## Line – Command Mode Page

Line – Command Mode Page Settings	Description
Mode	Select the method of enabling command mode or choose to disable command mode. Choices are:  <b>Always</b> = immediately enables command mode for the serial line. <b>Use Serial String</b> = enables command mode when the serial string is read on the serial line during boot time. <b>Disabled</b> = Disables command mode.
Wait Time	Enter the maximum number of milliseconds the selected serial line waits to receive the specific serial string at boot time to enter command mode. Default is 5000 milliseconds.
Serial String	Enter the serial string that places the serial line into command mode. After entering a string, use the buttons to indicate whether the string is a text or binary value.
Echo Serial String	Select whether the serial line echoes the specified serial string at boot time. Choices are:  <b>Yes</b> = echoes the characters specified in the <b>Serial String</b> text box. <b>No</b> = does not echo the characters specified in the <b>Serial String</b> text box.
Signon Message	Enter the boot-up signon message to be sent over the serial line at boot time. After entering the message, select whether the string is a text or binary value.

## Tunnel Pages

The Tunnel pages let you view and configure settings for tunnels. (For more information, see [Tunneling](#) on page 144.)

### To select a tunnel:

**EDS4100:** Click **Tunnel 1**, **Tunnel 2**, **Tunnel 3**, or **Tunnel 4** at the top of the page.

**EDS8/16/32PR:** Select the tunnel from the **Select Tunnel** drop-down list at the top of the page.

After you select a tunnel, you can click **Statistics**, **Serial Settings**, **Start/Stop Chars**, **Accept Mode**, **Connect Mode**, **Disconnect Mode**, **Packing Mode**, **Modem Emulation**, or **AES Keys** to view and change the settings of the selected tunnel. Because all tunnels operate independently, you can specify different configuration settings for each tunnel.

### Tunnel – Statistics Page

The Tunnel – Statistics page displays when you click **Tunnel** in the menu bar. It also displays when you click **Statistics** at the top of one of the other Tunnel pages. This read-only page shows the status and statistics for the tunnel currently selected at the top of this page.

Figure 7-5. Tunnel - Statistics Page

The screenshot shows the Lantronix EDS32PR web interface. The top left features the Lantronix logo, and the top right shows 'EDS32PR Powered by Evolution OS'. A left-hand navigation menu lists various system components. The main content area is titled 'Tunnel 1 - Statistics' and includes a 'Select Tunnel' dropdown menu currently set to 'Tunnel 1'. Below the dropdown are three buttons: 'Statistics', 'Serial Settings', and 'Start/Stop Chars'. Underneath these buttons are three columns of settings: 'Accept Mode', 'Connect Mode', and 'Disconnect Mode'; 'Packing Mode', 'Modem Emulation', and 'AES Keys'. The 'Statistics' button is active, displaying a table of aggregate counters. Below the table are sections for 'Connect Counters' and 'Accept Counters', both indicating 'There is no active connection.' A footer at the bottom of the page reads 'Copyright © Lantronix, Inc. 2005. All rights reserved.'

Aggregate Counters	
Completed Connects:	4
Completed Accepts:	0
Disconnects:	4
Dropped Connects:	1
Dropped Accepts:	0
Octets forwarded from Serial:	28
Octets forwarded from Network:	232
Connect Connection Time:	0 days 01:09:06.218
Accept Connection Time:	0 days 00:00:00.000
Connect DNS Address Changes:	0
Connect DNS Address Invalids:	0

Connect Counters  
There is no active connection.

Accept Counters  
There is no active connection.

## Tunnel – Serial Settings Page

If you click **Serial Settings** at the top of one of the Tunnel pages, the Tunnel – Serial Settings page displays. This page shows the settings for the tunnel selected at the top of the page and lets you change the settings. If you change the **Buffer Size** value, the EDS must be rebooted for the change to take effect. Changing the other values does not require a reboot.

Under **Current Configuration**, **Buffer Size** has a **Reset** link that lets you reset the buffer size value shown. If you click this link, a message tells you that you will have to reboot the EDS. Click **OK** to proceed or **Cancel** to cancel the operation.

Figure 7-6. Tunnel – Serial Settings Page

The screenshot shows the Lantronix EDS32PR web interface. The top header includes the Lantronix logo and 'EDS32PR Powered by Evolution OS'. A left-hand navigation menu lists various system settings like Status, Network, Line, Tunnel, DNS, etc. The main content area is titled 'Tunnel 1- Serial Settings' and features a 'Select Tunnel:' dropdown menu set to 'Tunnel 1'. Below this are several tabs: Statistics, Serial Settings (selected), Start/Stop Chars, Accept Mode, Connect Mode, Disconnect Mode, Packing Mode, Modem Emulation, and AES Keys. The configuration options include:
 

- Buffer Size: [input field]
- Read Timeout: [input field] milliseconds
- Wait For Read Timeout:  Enabled  Disabled
- A Submit button.

 A 'Current Configuration' table is shown below:
 

Line Settings:	RS232, 9600, N, 8, 1, None
Buffer Size:	2048bytes [Reset]
Read Timeout:	200milliseconds
Wait For Read Timeout:	Disabled

 On the right side, there is explanatory text:
 

- For Tunneling, the **Buffer Size** of the buffer used for reading data on the Serial Line can be modified. The valid size range is from 1 to 4096 bytes. Changing this value requires a reboot.
- A **Read Timeout** specifies how long to wait when waiting for incoming data on the Serial Line.
- The **Wait For Read Timeout** boolean specifies to wait the entire **Read Timeout** when waiting for incoming data on the Serial Line. The waiting occurs even if there is data in the read buffer ready to be processed. Only when the read buffer completely fills up is the **Read Timeout** ignored.

 The footer contains the copyright notice: Copyright © Lantronix, Inc., 2005. All rights reserved.

Tunnel – Serial Settings Page

Tunnel – Serial Settings Page	Description
Buffer Size	Enter the size of the buffer used to receive data on the serial line. Range = 1 to 4096 bytes. Default is 2048 bytes. Changing this value requires the EDS to be rebooted.
Read Timeout	Enter the maximum number of milliseconds that the EDS waits for incoming data on the serial line. Default is 200 milliseconds.
Wait for Read Timeout	<p>Select whether the EDS waits the entire Read Timeout value for incoming data on the serial line. Waiting occurs even if there is data in the read buffer ready to be processed. The Read Timeout is ignored only when the read buffer completely fills with data. Choices are:</p> <p><b>Enabled</b> = waits the entire Read Timeout value for incoming data on the serial line.</p> <p><b>Disabled</b> = does not wait the entire Read Timeout value for incoming data (<i>default</i>).</p>

## Tunnel – Start/Stop Characters Page

If you click **Start/Stop Chars** at the top of one of the Tunnel pages, the Tunnel – Start/Stop Chars page displays. This page shows the start and stop characters used for the tunnel selected at the top of the page and lets you change the settings for that tunnel.

Figure 7-7. Tunnel – Start/Stop Chars Page

LANTRONIX®
EDS32PR  
Powered by Evolution OS

- Status
- Network
- Line
- Tunnel
- DNS
- SNMP
- FTP
- TFTP
- Syslog
- HTTP
- CLI
- Email
- SSH
- SSL
- XML
- Filesystem
- Protocol Stack
- IP Address Filter
- Query Port
- Diagnostics
- System

Select Tunnel: Tunnel 1

Statistics
Serial Settings
Start/Stop Chars

Accept Mode
Connect Mode
Disconnect Mode

Packing Mode
Modem Emulation
AES Keys

### Tunnel 1- Start/Stop Chars

Start Character:

Stop Character:

Echo Start Character:  On  Off

Echo Stop Character:  On  Off

---

#### Current Configuration

Start Character:	<None>
Stop Character:	<None>
Echo Start Character:	Off
Echo Stop Character:	Off

The **Start Character**, when read on the Serial Line, can be used to initiate a new connection for a Tunnel in Connect Mode and enable a Tunnel in Accept Mode to start listening for connections.

The **Stop Character**, when read on the Serial Line, can be used to disconnect an active Tunnel connection.

Optionally, the **Start/Stop Characters** can be echoed (sent) or not echoed (not set) on the Tunnel when read on the Serial Line.

Copyright © Lantronix, Inc. 2005. All rights reserved.

## Tunnel – Start/Stop Chars Page

Tunnel – Start/Stop Chars Page Settings	Description
Start Character	Enter the start character. When this character is read on the serial line, it either initiates a new connection (for a tunnel in Connect mode) or enables a tunnel in Accept mode to start listening for connections. Default is <none>.
Stop Character	Enter the stop character. When this character is read on the serial line, it disconnects an active tunnel connection. Default is <none>.
Echo Start Character	<p>Select whether the start character is forwarded (or “echoed”) through the selected tunnel when the serial line is read. Choices are:</p> <p><b>On</b> = echo the start character on the selected tunnel when the serial line is read.</p> <p><b>Off</b> = do not echo the start character. (<i>default</i>)</p>
Echo Stop Character	<p>Select whether the stop character is echoed through the selected tunnel when the serial line is read. Choices are:</p> <p><b>On</b> = echo the stop character on the selected tunnel when the serial line is read.</p> <p><b>Off</b> = do not echo the stop character. (<i>default</i>)</p>

## Tunnel – Accept Mode Page

Accept Mode determines how the EDS “listens” for an incoming connection. If you click **Accept Mode** at the top of one of the Tunnel pages, the Tunnel – Accept Mode page displays. Here you can select the method for starting a tunnel in Accept mode and select other settings for the tunnel selected at the top of the page.

Under **Current Configuration**, **Local Port** has a **Reset** link if it has been changed from the default. If you click this link, a message tells you that your action may stop an active connection. Click **OK** to proceed or **Cancel** to cancel the operation.

For more information about Accept mode, see [Accept Mode](#) on page 146.



Figure 7-8. Tunnel – Accept Mode Page

LANTRONIX®

EDS32PR

Powered by Evolution OS

---

Status

Network

Line

Tunnel

DNS

SNMP

FTP

TFTP

Syslog

HTTP

CLI

Email

SSH

SSL

XML

Filesystem

Protocol Stack

IP Address Filter

Query Port

Diagnostics

System

Select Tunnel: Tunnel 1

Statistics
Serial Settings
Start/Stop Chars

Accept Mode
Connect Mode
Disconnect Mode

Packing Mode
Modem Emulation
AES Keys

### Tunnel 1- Accept Mode

**Mode:**  Disabled  Enabled  
 Any Character  Modem Control Asserted  
 Start Character  Modem Emulation

**Local Port:**

**Protocol:**  TCP  SSH  Telnet  TCP/AES

**Flush Serial Data:**  Enabled  Disabled

**Block Serial Data:**  On  Off

**Block Network Data:**  On  Off

**TCP Keep Alive:**  seconds

**Email on Connect:** None

**Email on Disconnect:** None

**Password:**

**Prompt for Password:**  On  Off

---

#### Current Configuration

<b>Mode:</b>	Disabled
<b>Local Port:</b>	10001
<b>Protocol:</b>	Tcp
<b>Flush Serial Data:</b>	Disabled
<b>Block Serial Data:</b>	Off
<b>Block Network Data:</b>	Off
<b>TCP Keep Alives:</b>	Default 45 seconds
<b>Email on Connect:</b>	<None>
<b>Email on Disconnect:</b>	<None>
<b>Password:</b>	<Not Configured> <a href="#">[Reset]</a>
<b>Prompt for Password:</b>	Off

A Tunnel in Accept Mode can be started in a number of ways:

**Disabled:** never started

**Enabled:** always started

**Any Character:** started when any character is read on the Serial Line

**Start Character:** started when the Start Character is read on the Serial Line

**Modem Control Asserted:** started when the Modem Control pin is asserted on the Serial Line

**Modem Emulation:** started when triggered by Modem Emulation. Connect mode must also be set to Modem Emulation

The **Local Port** can be overridden and by default is 10001 for Tunnel 1, 10002 for Tunnel 2, and so on.

The **Protocol** used on the connection can be one of TCP, SSH, Telnet, or TCP w/AES. If security is a concern it is highly recommended that SSH be used. When using SSH both the [SSH Server Host Keys](#) and [SSH Server Authorized Users](#) must be configured.

The **Flush Serial Data** boolean specifies to flush the Serial Line when a connection is made.

For debugging purposes, the **Block Serial Data** and **Block Network Data** booleans can be toggled to discard all incoming data on the respective interface.

The **TCP Keep Alive** timer specifies how often to probe the remote host in order to keep the TCP connection up during idle transfer periods. Enter 0 to disable.

The **Password** can be up to 31 characters in length and must contain only alphanumeric characters and punctuation. When set, clients must send the correct password string to the unit within 30 seconds from opening network connection in order to enable data transmission. The password sent to the unit must be terminated with one of the following: (a) 0x10 (LF), (b) 0x00, (c) 0x13 0x10 (CR LF) (d) 0x13 0x00. If Prompt for Password is set to On, user will be prompted for password upon connection.

Copyright © Lantronix, Inc., 2005. All rights reserved.

## Tunnel – Accept Mode Page

Tunnel – Accept Mode Page Settings	Description
Mode	<p>Select the method used to start a tunnel in Accept mode. Choices are:</p> <p><b>Disabled</b> = do not accept an incoming connection.</p> <p><b>Enabled</b> = accept an incoming connection. (<i>default</i>)</p> <p><b>Any Character</b> = start waiting for an incoming connection when any character is read on the serial line.</p> <p><b>Start Character</b> = start waiting for an incoming connection when the start character for the selected tunnel is read on the serial line.</p> <p><b>Modem Control Asserted</b> = start waiting for an incoming connection as long as the Modem Control pin (DSR) is asserted on the serial line until a connection is made.</p> <p><b>Modem Emulation</b> = start waiting for an incoming connection when triggered by modem emulation AT commands. Connect mode must also be set to <b>Modem Emulation</b> (see <a href="#">Tunnel – Connect Mode</a> on page 59).</p>
Local Port	<p>Enter the number of the local port used to receive (or listen for) packets.</p> <p>Default is 10001 for Tunnel 1, 10002 for Tunnel 2, and so forth.</p>
Protocol	<p>Select the protocol to be used on the connection. Choices are:</p> <p><b>TCP</b> (<i>default</i>)</p> <p><b>SSH</b> = use this setting if security is a concern. When using SSH, both the SSH Server Host Keys and SSH Server Authorized Users must be configured. (See <a href="#">SSH</a> on page 143.)</p> <p><b>Telnet</b></p> <p><b>TCP/AES</b> = use for secure tunneling between two EDS's or software that supports AES such as the Secure Com Port Redirector. Secure Com Port Redirector is on the CD that came with your EDS or on the Lantronix Web Site (<a href="http://www.lantronix.com">www.lantronix.com</a>).</p>
Flush Serial Drive	<p>Select whether the serial line is flushed when a connection is made. Choices are:</p> <p><b>Enabled</b> = flush the serial line when a connection is made.</p> <p><b>Disabled</b> = do not flush the serial line. (<i>default</i>)</p>
Block Serial Data	<p>Select whether incoming serial data should be discarded. This setting is used for debugging purposes. Choices are:</p> <p><b>On</b> = discard all incoming serial data on the respective interface.</p> <p><b>Off</b> = do not discard all incoming serial data. (<i>default</i>)</p>
Block Network Data	<p>Select whether incoming network data should be discarded. This setting is used for debugging purposes. Choices are:</p> <p><b>On</b> = discard all incoming network data on the respective interface.</p> <p><b>Off</b> = do not discard all incoming network data. (<i>default</i>)</p>
TCP Keep Alive	<p>Specify the number of milliseconds the EDS waits during an inactive connection before checking the status of the connection. If the EDS does not receive a response from the remote host, it drops that connection.</p>

Tunnel – Accept Mode Page Settings	Description
Email on Connect	Select whether an email is sent when a connection is made. <b>None</b> = do not send an email. <b>Email #</b> = send an email corresponding to the tunnel number.
Email on Disconnect	Select whether an email corresponding to the tunnel number is sent when a connection is closed. <b>None</b> = do not send an email. <b>Email #</b> = send an email corresponding to the tunnel number.
Password	Enter a password that clients must send to the EDS within 30 seconds from opening a network connection to enable data transmission.  The password can have up to 31 characters and must contain only alphanumeric characters and punctuation. When set, the password sent to the EDS must be terminated with one of the following: (a) 0x10 (LF), (b) 0x00, (c) 0x13 0x10 (CR LF), or (d) 0x13 0x00.
Prompt for Password	Indicate whether the user should be prompted for the password upon connection.  <b>On</b> = prompt for a password upon connection. <b>Off</b> = do not prompt for a password upon connection.

## Tunnel – Connect Mode Page

Connect Mode determines how the EDS initiates a connection to a remote host or device. If you click **Connect Mode** at the top of one of the Tunnel pages, the Tunnel – Connect Mode page displays. Here you can select the method for starting a tunnel in Connect mode and select other settings for the tunnel selected at the top of the page.

Any configuration changes you make on the displayed page apply to the tunnel you selected at the top of this page. For example, if **Tunnel 1** is selected, any configuration changes you make apply to tunnel 1.

Under **Current Configuration**, both **Remote Address** and **Remote Port** have a **Delete** link that lets you delete the remote address and port number shown. If you click this link, a message tells you that your action may stop an active connection. Click **OK** to proceed or **Cancel** to cancel the operation.

For more information about Connect mode, see [Connect Mode](#) on page 145.

Figure 7-9. Connect Mode Page

LANTRONIX®
EDS32PR  
Powered by Evolution OS

- Status
- Network
- Line
- Tunnel
- DNS
- SNMP
- FTP
- TFTP
- Syslog
- HTTP
- CLI
- Email
- SSH
- SSL
- XML
- Filesystem
- Protocol Stack
- IP Address Filter
- Query Port
- Diagnostics
- System

Select Tunnel: Tunnel 1

---

Statistics

Accept Mode

Packing Mode

Serial Settings

**Connect Mode**

Modem Emulation

Start/Stop Chars

Disconnect Mode

AES Keys

### Tunnel 1- Connect Mode

**Mode:**  Disabled  Enabled

Any Character  Modem Control Asserted

Start Character  Modem Emulation

**Remote Address:**

**Remote Port:**

**Local Port:**

**Protocol:**  TCP  UDP  SSH  
 TCP/AES  UDP/AES

**Reconnect Timer:**  milliseconds

**Flush Serial Data:**  Enabled  Disabled

**SSH Username:**

**Block Serial Data:**  On  Off

**Block Network Data:**  On  Off

**TCP Keep Alive:**  seconds

**Email on Connect:** None

**Email on Disconnect:** None

---

#### Current Configuration

<b>Mode:</b>	Disabled
<b>Remote Address:</b>	172.18.11.116[Delete]
<b>Remote Port:</b>	23[Delete]
<b>Local Port:</b>	Random
<b>Protocol:</b>	Tcp
<b>Reconnect Timer:</b>	15000milliseconds
<b>Flush Serial Data:</b>	Disabled
<b>SSH Username:</b>	<None>
<b>Block Serial Data:</b>	Off
<b>Block Network Data:</b>	Off
<b>TCP Keep Alives:</b>	Default 45 seconds
<b>Email on Connect:</b>	<None>
<b>Email on Disconnect:</b>	<None>

A Tunnel in Connect Mode can be started in a number of ways:

**Disabled:** never started

**Enabled:** always started

**Any Character:** started when any character is read on the Serial Line

**Start Character:** started when the Start Character is read on the Serial Line

**Modem Control Asserted:** started when the Modem Control pin is asserted on the Serial Line

**Modem Emulation:** started when triggered by Modem Emulation

The **Remote Address** and **Remote Port** specifies the remote host to connect to. The **Local Port** is by default random but can be overridden.

The **Protocol** used on the connection can be one of TCP, UDP, SSH, TCP w/AES, or UDP w/AES. If security is a concern it is highly recommended that SSH be used. The **SSH Username** specifies the **SSH Client User** to use for an SSH connection.

The **Reconnect Timer** specifies how long to wait before trying to reconnect to the remote host after a previous attempt failed or connection was closed.

The **Flush Serial Data** boolean specifies to flush the Serial Line when a connection is made.

For debugging purposes, the **Block Serial Data** and **Block Network Data** booleans can be toggled to discard all incoming data on the respective interface.

The **TCP Keep Alive** timer specifies how often to probe the remote host in order to keep the TCP connection up during idle transfer periods. Enter 0 to disable.

Copyright © Lantronix, Inc. 2005. All rights reserved.

## Tunnel – Connect Mode Page

Tunnel – Connect Mode Page Settings	Description
Mode	<p>Select the method to be used to start a connection to a remote host or device. Choices are:</p> <p><b>Disabled</b> = an outgoing connection is never started. (<i>default</i>)</p> <p><b>Enabled</b> = a connection is attempted until one is made. If the connection gets disconnected, the EDS retries until a connection is made.</p> <p><b>Any Character</b> = a connection is started when any character is read on the serial line.</p> <p><b>Modem Control Asserted</b> = a connection is attempted as long as the Modem Control pin (DSR) is asserted until a connection is made.</p> <p><b>Start Character</b> = a connection is attempted when the start character for the selected tunnel is read on the serial line.</p> <p><b>Modem Emulation</b> = a connection is started when triggered by modem emulation AT commands.</p>
Remote Address	Enter the address of the remote host to which the selected tunnel will connect. Default is <none>.
Remote Port	Enter the number of the remote port to which the selected tunnel will connect. Default is <none>.
Local Port	Enter the number of the local port that will participate in this tunnel. Default is Port 1 = 10001, Port 2 = 10002, Port 3 = 10002, and Port 4 = 10004, and so forth.
Protocol	<p>Select the protocol to use on the connection. Choices are:</p> <p><b>TCP</b> (<i>default</i>)</p> <p><b>UDP</b></p> <p><b>SSH</b> = use this setting if security is a concern. This setting requires you to enter an SSH username.</p> <p><b>TCP/AES</b> = use for secure tunneling by means of TCP between two EDS devices or other devices that support AES.</p> <p><b>UDP/AES</b> = use for secure tunneling by means of UDP between two EDS devices or other devices that support AES.</p>
Reconnect Timer	Enter the maximum number of milliseconds to wait before trying to reconnect to the remote host after a previous attempt failed or the connection was closed. Default is 15000 milliseconds.
Flush Serial Data	<p>Select whether to flush the serial line when a connection is made. Choices are:</p> <p><b>Enabled</b> = flush the serial line when a connection is made.</p> <p><b>Disabled</b> = do not flush the serial line. (<i>default</i>)</p>
SSH Username	If you selected SSH as the protocol for this tunnel, enter the SSH client user that is to be used for the SSH connection. Default is <none>.

Tunnel – Connect Mode Page Settings	Description
Block Serial Data	<p>Select whether incoming block serial data should be discarded. This setting is used for debugging purposes. Choices are:</p> <p><b>On</b> = discard all incoming serial data on the respective interface.</p> <p><b>Off</b> = do not discard all incoming serial data. (<i>default</i>)</p>
Block Network Data	<p>Select whether incoming block network data should be discarded. This setting is used for debugging purposes. Choices are:</p> <p><b>On</b> = discard all incoming network data on the respective interface.</p> <p><b>Off</b> = do not discard all incoming network data. (<i>default</i>)</p>
TCP Keep Alive	<p>Specifies the number of milliseconds the EDS waits during an inactive connection before checking the status of the connection. If the EDS does not receive a response from the remote host, it drops that connection.</p>
Email on Connect	<p>Select whether email should be sent when a connection is made.</p> <p><b>None</b> = no email should be sent.</p> <p><b>Email #</b> = send an email corresponding to the tunnel number.</p>
Email on Disconnect	<p>Select whether email should be sent when a connection is closed.</p> <p><b>None</b> = do not send an email</p> <p><b>Email #</b> = send an email corresponding to the tunnel number.</p>

## Tunnel – Disconnect Mode Page

If you click **Disconnect Mode** at the top of one of the Tunnel pages, the Tunnel – Disconnect Mode page displays. Here you can select the disconnect method for the tunnel selected at the top of the page. For more information about Disconnect mode, see [Disconnect Mode](#) on page 146.

Figure 7-10. Tunnel – Disconnect Mode Page

**LANTRONIX®** **EDS32PR**  
Powered by **Evolution OS**

Status  
Network  
Line  
Tunnel  
DNS  
SNMP  
FTP  
TFTP  
Syslog  
HTTP  
CLI  
Email  
SSH  
SSL  
XML  
Filesystem  
Protocol Stack  
IP Address Filter  
Query Port  
Diagnostics  
System

Select Tunnel: Tunnel 1

Statistics Serial Settings Start/Stop Chars  
Accept Mode Connect Mode **Disconnect Mode**  
Packing Mode Modem Emulation AES Keys

### Tunnel 1- Disconnect Mode

Mode:  Disabled  Timeout  
 Stop Character  Modem Control Not Asserted

Timeout:  milliseconds

Flush Serial Data:  Enabled  Disabled

#### Current Configuration

Mode:	Disabled
Timeout:	60000milliseconds
Flush Serial Data:	Disabled

A Tunnel can be configured to Disconnect in a number of ways:  
**Disabled:** never disconnected  
**Timeout:** disconnect after idle timeout occurs  
**Stop Character:** disconnect when the Stop Character is read on the Serial Line  
**Modem Control Not Asserted:** disconnect when Modem Control pin is not asserted on the Serial Line  
The **Timeout** specifies the idle time on a connection that must pass before a Tunnel is disconnected.  
The **Flush Serial Data** boolean specifies to flush the Serial Line when the Tunnel is disconnected.

Copyright © Lantronix, Inc. 2005. All rights reserved.

Tunnel – Disconnect Mode Page

Tunnel – Disconnect Mode Page Settings	Description
Mode	Select the method used to disconnect an active tunnel connection. Choices are:  <b>Disabled</b> = an active connection is never disconnected. ( <i>default</i> ) <b>Timeout</b> = an active connection is disconnected after the specified idle time elapses. <b>Stop Character</b> = an active connection is disconnected when the specified stop character is read on the serial line. <b>Modem Control Not Asserted</b> = an active connection is disconnected when the Modem Control pin (DSR) is de-asserted on the serial line.
Timeout	Enter the idle time, in milliseconds, that must elapse for a connection before it is disconnected. Default is 60000 milliseconds.
Flush Serial Data	Select whether the serial line should be flushed when a connection is disconnected. Choices are:  <b>Enabled</b> = flush the serial line when a connection is disconnected. <b>Disabled</b> = do not flush the serial line. ( <i>default</i> )

## Tunnel – Packing Mode Page

When tunneling, data can be packed (queued) and sent in large chunks on the network instead of being sent immediately after being read on the serial line. If you click **Packing Mode** at the top of one of the Tunnel pages, the Tunnel – Packing Mode page displays. Here you can select packing settings for the tunnel selected at the top of the page. For more information about Packing mode, see [Packing Mode](#) on page 147.

Figure 7-11. Tunnel – Packing Mode Page

LANTRONIX®
EDS32PR  
Powered by Evolution OS

Status

Network

Line

Tunnel

DNS

SNMP

FTP

TFTP

Syslog

HTTP

CLI

Email

SSH

SSL

XML

Filesystem

Protocol Stack

IP Address Filter

Query Port

Diagnostics

System

Select Tunnel: Tunnel 1

---

Statistics
Serial Settings
Start/Stop Chars

Accept Mode
Connect Mode
Disconnect Mode

Packing Mode
Modem Emulation
AES Keys

### Tunnel 1- Packing Mode

**Mode:**             Disabled         Timeout  
 Send Character

**Timeout:**         milliseconds

**Threshold:**    

**Send Character:**

**Trailing Character:**

---

#### Current Configuration

<b>Mode:</b>	Disabled
<b>Timeout:</b>	1000 milliseconds
<b>Threshold:</b>	512 bytes
<b>Send Character:</b>	<None>
<b>Trailing Character:</b>	<None>

When Tunneling, instead of sending data on the network immediately after being read on the Serial Line, the data can be packed (queued) and sent in larger chunks.

A Tunnel can be configured to use Packing Mode in a number of ways:

**Disabled:** data never packed

**Timeout:** data sent after timeout occurs

**Send Character:** data sent when the Send Character is read on the Serial Line

The **Threshold** specifies if the amount of queued data reaches this limit, then send the data on the network immediately.

The **Timeout** specifies how long to wait before sending the queued data on the network.

If used, the **Send Character** is a special character that when read on the Serial Line forces the queued data to be sent out immediately.

The **Trailing Character** is a special character that is injected into the outgoing data stream right after the **Send Character**.

Copyright © Lantronix, Inc. 2005. All rights reserved.



## Tunnel – Packing Mode Page

Tunnel – Packing Mode Page Settings	Description
Mode	Select the method used to pack data. Choices are: <b>Disabled</b> = data is never packed. ( <i>default</i> ) <b>Timeout</b> = data is sent after the timeout elapses. <b>Send Character</b> = data is sent when the send character is read on the serial line.
Timeout	Enter the maximum number of milliseconds to wait before sending queued data across the network. Default is 1000 milliseconds.
Threshold	Enter the queued data limit that, when reached, immediately sends queued data to the network. Default is 512 bytes.
Send Character	Enter the send character. When this character is read on the serial line, it forces the queued data to be sent immediately. Default is <none>.
Trailing Character	Enter the trailing character. This character is inserted into the outgoing data stream immediately after the send character. Default is <none>.

## Tunnel – Modem Emulation Page

A tunnel in connect mode can be initiated using modem commands incoming from the serial line. If you click **Modem Emulation** at the top of one of the Tunnel pages, the Tunnel – Modem Emulation page displays. Here you can select modem emulation settings for the tunnel selected at the top of the page. For more information about modem emulation, see [Modem Emulation](#) on page 147.

Tunnel – Modem Emulation Page

LANTRONIX®
EDS32PR  
Powered by Evolution OS

- Status
- Network**
- Line
- Tunnel
- DNS
- SNMP
- FTP
- TFTP
- Syslog
- HTTP
- CLI
- Email
- SSH
- SSL
- XML
- Filesystem
- Protocol Stack
- IP Address Filter
- Query Port
- Diagnostics
- System

Select Tunnel: Tunnel 1

---

Statistics
Serial Settings
Start/Stop Chars

Accept Mode
Connect Mode
Disconnect Mode

Packing Mode
Modem Emulation
AES Keys

### Tunnel 1- Modem Emulation

Echo Pluses:  On  Off

Echo Commands:  On  Off

Verbose Response Codes:  On  Off

Response Codes:  Text  Numeric

Error Unknown Commands:  On  Off

Connect String:

---

#### Current Configuration

Echo Pluses:	On
Echo Commands:	On
Verbose Response Codes:	On
Response Codes:	Text
Error Unknown Commands:	On
Optional Connect String:	<None>

A Tunnel in Connect Mode can be initiated using Modem commands incoming from the Serial Line.

The **Modem Pluses** and **Modem Commands** can be echoed (sent) or not echoed (not sent) on the Tunnel when read on the Serial Line.

The **Verbose Response Codes** boolean specifies whether or not Modem Response Codes are sent out on the Serial Line.

The **Response Codes** value specifies if the Modem Response Codes sent out on the Serial Line should be sent in 'Text' or 'Numeric' representation.

The **Error Unknown Commands** value specifies if an ERROR return value should be sent on unrecognized AT commands. If 'on' then ERROR is returned for unrecognized AT commands otherwise if 'off' then OK is returned for unrecognized AT commands.

The **Connect String** is a customized string that is sent with the CONNECT Modem Response Code.

Copyright © Lantronix, Inc. 2005. All rights reserved.

## Tunnel – Modem Emulation Page

Tunnel – Modem Emulation Page Settings	Description
Echo Pluses	Select whether the modem plus (+) command is echoed (sent). Choices are: <b>On</b> = modem pluses are echoed. <b>Off</b> = modem pluses are not echoed. ( <i>default</i> )
Echo Commands	Select whether modem commands are echoed on the serial line. Choices are: <b>On</b> = modem commands are echoed. ( <i>default</i> ) <b>Off</b> = modem commands are not echoed.
Verbose Response Codes	Select whether modem response (result) codes are sent on the serial line. Choices are: <b>Text</b> = modem responses are sent on the serial line. ( <i>default</i> ) <b>Numeric</b> = modem responses are not sent.
Response Codes	Select whether modem response (result) codes sent on the serial line take the form of words or numbers. Choices are: <b>Text</b> = modem responses are sent as words. ( <i>default</i> ) <b>Numeric</b> = modem responses are sent as numbers.
Error Unknown Commands	Select whether an ERROR or OK response is sent in reply to unrecognized AT commands. Choices are: <b>On</b> = ERROR is returned for unrecognized AT commands. <b>Off</b> = OK is returned for unrecognized AT commands. ( <i>default</i> )
Connect String	If required, enter a customized string that is sent along with the CONNECT response code. Default is <none>.

## Tunnel – AES Keys Page

Four Advanced Encryption Standard (AES) Encryption Keys are used for tunneling. Connect mode and Accept mode contain their own sets of keys. One key is used for encrypting outgoing data and another key is used for decrypting incoming data. These AES keys are fixed at 16 bytes. Any keys entered that are less than 16 bytes long are padded with zeroes.

If you click **AES Keys** at the top of one of the Tunnel pages, the Tunnel – AES Keys page displays. Here you can enter key data as text or binary values for the tunnel selected at the top of the page. Binary values are a string of characters representing hexadecimal or decimal values.

**Note:** Keys are shared secret keys that must be known by both sides of the connection and kept secret.

**Note:** Tunneling using AES encryption uses a non-standard protocol and shared keys, making it not very secure. The EDS also supports SSH as an alternative method of secure tunneling. SSH tunneling has the advantage of not using shared keys.

Figure 7-12. Tunnel – AES Keys Page

The screenshot shows the LANTRONIX EDS32PR web interface. The top header includes the LANTRONIX logo and 'EDS32PR Powered by Evolution OS'. A left-hand navigation menu lists various system settings like Network, Line, Tunnel, DNS, etc. The main content area is titled 'Tunnel - AES Keys' and is for 'Tunnel 1'. It features two main sections: 'Accept Mode AES Keys' and 'Connect Mode AES Keys'. Each section has input fields for 'Encrypt Key' and 'Decrypt Key', with radio buttons to select between 'Text' and 'Binary' formats. A 'Submit' button is located below the Connect Mode section. At the bottom, a 'Current Configuration' table shows the current state of the keys. On the right side, there is a detailed help text explaining that AES keys are 16 bytes long and that the keys are shared secrets.

Accept Mode AES Keys	
Encrypt Key:	<None>
Decrypt Key:	<None>
Connect Mode AES Keys	
Encrypt Key:	<None>
Decrypt Key:	<None>

## Tunnel – AES Keys Page

Tunnel – AES Keys Page Settings	Description
Accept Mode AES Keys: Encrypt Key	Enter the AES encrypt key for Accept mode. After entering a value, select an option to specify whether the value is text or binary. Default is <none>.
Accept Mode AES Keys: Decrypt Key	Enter the AES decrypt key for Accept mode. After entering a value, select an option to specify whether the value is text or binary. Default is <none>.
Connect Mode AES Keys: Encrypt Key	Enter the AES encrypt key for Connect mode. After entering a value, select an option to specify whether the value is text or binary. Default is <none>.
Connect Mode AES Keys: Decrypt Key	Enter the AES decrypt key for Connect mode. After entering a value, select an option to specify whether the value is text or binary. Default is <none>.

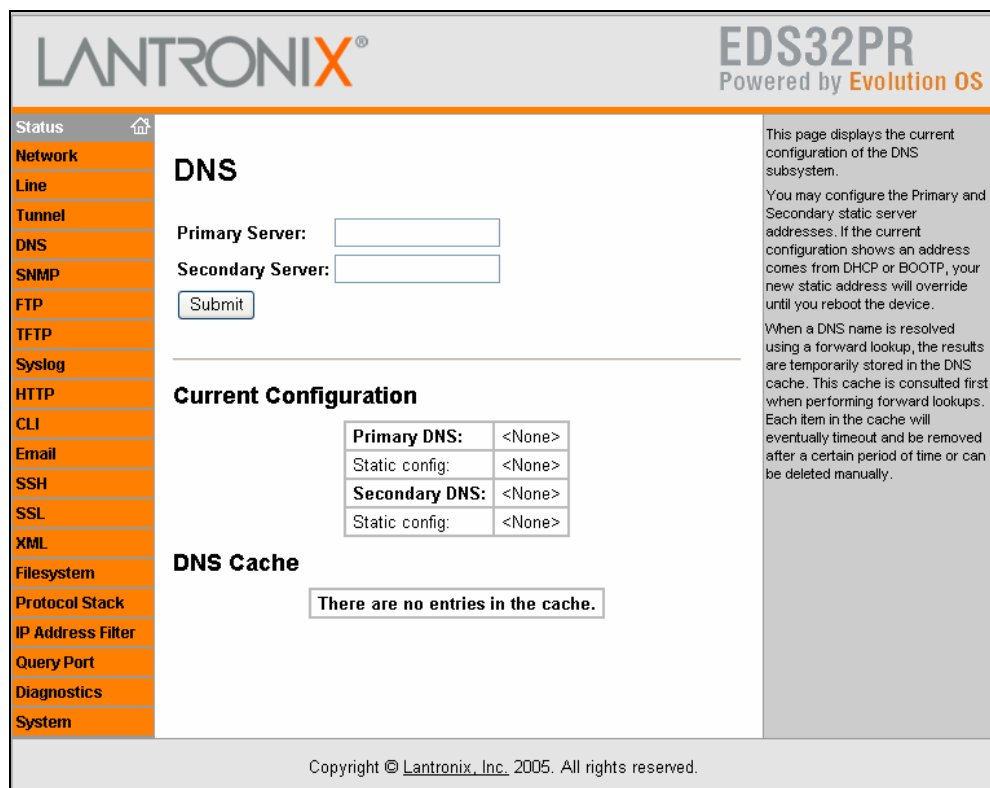
## 8: Services Settings

### DNS Page


Clicking the **DNS** link in the menu bar displays the DNS page. This page displays configuration settings for the domain name system (DNS) and lets you change them as necessary.

The DNS page also shows any contents in the DNS cache. When a DNS name is resolved using a forward lookup, the results are stored in the DNS cache temporarily. The EDS consults this cache when performing forward lookups. Each item in the cache eventually times out and is removed automatically after a certain period, or you can delete it manually.

Figure 8-1. DNS Page



**LANTRONIX®** EDS32PR  
Powered by Evolution OS

Status   
Network  
Line  
Tunnel  
DNS  
SNMP  
FTP  
TFTP  
Syslog  
HTTP  
CLI  
Email  
SSH  
SSL  
XML  
Filesystem  
Protocol Stack  
IP Address Filter  
Query Port  
Diagnostics  
System

### DNS

Primary Server:   
Secondary Server:

---

#### Current Configuration

Primary DNS:	<None>
Static config:	<None>
Secondary DNS:	<None>
Static config:	<None>

#### DNS Cache

There are no entries in the cache.

This page displays the current configuration of the DNS subsystem.  
You may configure the Primary and Secondary static server addresses. If the current configuration shows an address comes from DHCP or BOOTP, your new static address will override until you reboot the device.  
When a DNS name is resolved using a forward lookup, the results are temporarily stored in the DNS cache. This cache is consulted first when performing forward lookups. Each item in the cache will eventually timeout and be removed after a certain period of time or can be deleted manually.

Copyright © Lantronix, Inc. 2005. All rights reserved.

**Note:** If the current configuration shows an address comes from DHCP or BOOTP, the new static address overrides it until you reboot the device.

## DNS Page

DNS Page Settings	Description
Primary Server	Enter the DNS primary server that maintains the master zone information/file for a domain. Default is <none>.
Secondary Server	Enter the DNS secondary server that backs up the primary DNS server for a zone. Default is <none>.

## SNMP Page

Clicking the **SNMP** link in the menu bar displays the SNMP page. This page is used to configure the Simple Network Management Protocol (SNMP) agent. Using this page, you can configure the SNMP service to send a trap when it receives a request for information that contains an incorrect community name and does not match an accepted system name for the service.

Under **Current Configuration**, several settings have a **Delete** link that lets you delete these settings. If you click these links, a message asks whether you are sure you want to delete this information. Click **OK** to proceed or **Cancel** to cancel the operation.

Figure 8-2. SNMP Page

LANTRONIX® EDS32PR Powered by Evolution OS

Status [Home](#)

Network **SNMP**

Line

Tunnel

DNS

SNMP

FTP

TFTP

Syslog

HTTP

CLI

Email

SSH

SSL

XML

Filesystem

Protocol Stack

IP Address Filter

Query Port

Diagnostics

System

This page displays the current configuration of the SNMP Agent.

### SNMP

SNMP Agent:  On  Off

Read Community:

Write Community:

System Contact:

System Name:

System Description:

System Location:

Enable Traps:  On  Off

Primary TrapDest IP:

Secondary TrapDest IP:

---

#### Current Configuration

SNMP Agent Status:	Running (On)
Read Community:	<Configured>[Delete]
Write Community:	<Configured>[Delete]
System Contact:	Gary[Delete]
System Name:	EDS32PR_Gary[Delete]
System Description:	Serial/Ethernet Device[Delete]
System Location:	Tech Support[Delete]
Traps Enabled:	On
Primary TrapDest IP:	172.18.11.114[Delete]
Secondary TrapDest IP:	<None>

Copyright © Lantronix, Inc., 2005. All rights reserved.

## SNMP Page

SNMP Page Settings	Description
SNMP Agent	Select whether SNMP is enabled. Choices are: <b>On</b> = SNMP is enabled. ( <i>default</i> ) <b>Off</b> = SNMP is disabled.
Read Community	Enter the case-sensitive community name from which the EDS will receive trap messages. Default is public. For security, the read community name displays as <Configured> to show that one is enabled.
Write Community	Enter the case-sensitive community name to which the EDS will send trap messages. Default is private. For security, the write community name displays as <Configured> to show that one is enabled.
System Contact	Enter the name of the system contact. Default is <None>.
System Name	Enter the EDS's name.
System Description	Enter a system description for the EDS.
System Location	Enter the geographic location of the EDS. Default is <None>.
Enable Traps	Select whether SNMP cold start trap messages are enabled at boot. Choices are: <b>On</b> = SNMP cold start trap messages are enabled at boot time. ( <i>default</i> ) <b>Off</b> = SNMP traps are disabled.
Primary TrapDest IP	Enter the primary SNMP trap host. Default is <None>.
Secondary TrapDest IP	Enter the secondary SNMP trap host. Default is <None>.

## FTP Page

Clicking the **FTP** link in the menu bar displays the FTP page. This page displays the current File Transfer Protocol (FTP) connection status and various statistics about the FTP server.

Under **Current FTP Configuration and Statistics**, **FTP Password** has a **Reset** link that lets you reset the FTP password. If you click this link, a message asks whether you are sure you want to reset this information. Click **OK** to proceed or **Cancel** to cancel the operation.



Figure 8-3. FTP Page

LANTRONIX® EDS32PR  
Powered by Evolution OS

Status **Network** Line Tunnel DNS SNMP **FTP** TFTP Syslog HTTP CLI Email SSH SSL XML Filesystem Protocol Stack IP Address Filter Query Port Diagnostics System

## FTP

FTP Server:  On  Off

Username:

Password:

This page displays the current connection status and various statistics for the FTP Server.

### Current FTP Configuration and Statistics

FTP Status:	On (running)
FTP Username:	admin
FTP Password:	<Configured>[Reset]
Connections Rejected:	0
Connections Accepted:	0
Active Connections:	0
Last Client:	No device has connected

Copyright © Lantronix, Inc. 2005. All rights reserved.

### FTP Page

FTP Page Settings	Description
FTP Server	Select whether the FTP server is enabled. Choices are: <b>On</b> = FTP server is enabled. ( <i>default</i> ) <b>Off</b> = FTP server is disabled.
FTP Username	Enter the username required to gain FTP access. Default is admin.
FTP Password	Enter the password associated with the username.

## TFTP Page

Clicking the **TFTP** link in the menu bar displays the TFTP page. This page displays the status and various statistics about the Trivial File Transfer Protocol (TFTP) server.

Figure 8-4. TFTP Page

The screenshot shows the TFTP configuration page in the Lantronix EDS32PR web interface. The page has a header with the Lantronix logo and 'EDS32PR Powered by Evolution OS'. A left sidebar contains a menu with items like Status, Network, Line, Tunnel, DNS, SNMP, FTP, TFTP, Syslog, HTTP, CLI, Email, SSH, SSL, XML, Filesystem, Protocol Stack, IP Address Filter, Query Port, Diagnostics, and System. The main content area is titled 'TFTP' and contains two radio button settings: 'TFTP Server' (set to On) and 'Allow TFTP File Creation' (set to Off), with a 'Submit' button below. Below these settings is a section titled 'Current TFTP Configuration and Statistics' containing a table with the following data:

TFTP Status:	On (running)
TFTP File Creation:	Disabled
Files Downloaded:	0
Files Uploaded:	0
File Not Found Errors:	0
File Read Errors:	0
File Write Errors:	0
Unknown Errors:	0
Last Client:	No device has connected

On the right side of the page, there is a text box explaining the 'Allow TFTP File Creation' setting: 'This page displays the current status and various statistics for the TFTP Server. The Allow TFTP File Creation boolean specifies whether or not the TFTP Server can create a file if it does not already exist. Be careful when turning this feature on as it opens the device up to possible Denial-of-Service (DoS) attacks against the filesystem.'

At the bottom of the page, there is a copyright notice: 'Copyright © Lantronix, Inc. 2005. All rights reserved.'

### TFTP Page

TFTP Page Settings	Description
TFTP Server	Select whether the TFTP server is enabled. Choices are: <b>On</b> = TFTP server is enabled. ( <i>default</i> ) <b>Off</b> = TFTP server is disabled.
Allow TFTP File Creation	Select whether the TFTP server can create a file if it does not already exist. If you enable this feature, it exposes the EDS to possible Denial-of-Service (DoS) attacks against the filesystem. Choices are: <b>On</b> = files can be created by the TFTP server. <b>Off</b> = files cannot be created by the TFTP server. ( <i>default</i> )

## Syslog Page

Clicking the **Syslog** link in the menu bar displays the Syslog page. This page shows the current configuration, status, and statistics for the syslog. Here you can configure the syslog destination and the severity of the events to log.

Figure 8-5. Syslog Page

The screenshot shows the Syslog configuration page for a Lantronix EDS32PR device. The page includes a navigation menu on the left with 'Syslog' selected. The main content area has a 'Syslog' section with radio buttons for 'On' and 'Off', input fields for 'Host', 'Local Port', and 'Remote Port', and a dropdown for 'Severity To Log'. Below this is a table titled 'Current Syslog Configuration and Statistics' showing 'Syslog Status: Off (not running)', 'Host: <None>', 'Local Port: 514', 'Remote Port: 514', 'Severity Level: <None>', 'Messages Sent: 0', and 'Messages Failed: 0'. A copyright notice is at the bottom.

### Syslog Page

Syslog Page Settings	Description
Host	Enter the IP address of the remote server to which system logs are sent for storage.
Local Port	Enter the number of the local port on the EDS to which system logs are sent.  The system log is always saved to local storage, but it is not retained through reboots. Saving the system log to a server that supports remote logging services (see RFC 3164) allows the administrator to save the complete system log history. The default is 514.
Remote Port	Enter the number of the port on the remote server that supports logging services. The default is 514.

Syslog Page Settings	Description
Severity to Log	From the drop-down box, select the minimum level of system message the EDS should log. This setting applies to all syslog facilities. The drop-down list is in descending order of severity (e.g., Emergency is more severe than Alert.)

## HTTP Pages

Clicking the **HTTP** link in the menu bar displays the HTTP Statistics page. This page has four links at the top for viewing statistics and for viewing and changing configuration, authentication, and RSS settings.

### HTTP Statistics Page

The HTTP Statistics page displays when you click **HTTP** in the menu bar. It also displays when you click **Statistics** at the top of one of the other HTTP pages. This read-only page shows various statistics about the Hyper Text Transfer Protocol (HTTP) server.

**Note:** The HTTP log is a scrolling log, with the last Max Log Entries cached and viewable. To change the maximum number of entries that can be viewed, go to the HTTP Configuration page (described on page 77).

Figure 8-6. HTTP Statistics Page

The screenshot shows the EDS32PR interface with the following elements:

- Header:** LANTRONIX® logo on the left, and EDS32PR Powered by Evolution OS on the right.
- Left Navigation Menu:** A vertical list of menu items including Status, Network, Line, Tunnel, DNS, SNMP, FTP, TFTP, Syslog, HTTP, CLI, Email, SSH, SSL, XML, Filesystem, Protocol Stack, IP Address Filter, Query Port, Diagnostics, and System.
- Top Navigation Bar:** A horizontal bar with buttons for Statistics, Configuration, Authentication, and RSS.
- Main Content Area:**
  - HTTP Statistics:** A table showing various metrics:

Rx Bytes	20753
Tx Bytes	104799
200 - OK	36
400 - Bad Request	0
401 - Authorization Required	0
404 - Not Found	0
408 - Request Timeout	0
413 - Request Too Large	0
501 - Not Implemented	0
Status Unknown	0
Work Queue Full	0
Socket Error	0
Memory Error	0
Logs:	36 entries (5854 bytes) [View] [Clear]
- Right Sidebar:** Text explaining that the page displays HTTP Server statistics and that the HTTP Log is a scrolling log where only the last Max Log Entries are cached and viewable. It also mentions that the maximum number of entries can be modified on the HTTP Configuration page.
- Footer:** Copyright © Lantronix, Inc. 2005. All rights reserved.

## HTTP Configuration Page

If you click **Configuration** at the top of one of the HTTP pages, the HTTP Configuration page displays. Here you can change HTTP configuration settings.

Under **Current Configuration**, **Logs** has **View** and **Clear** links that let you view or clear the log. If you click **View**, the log displays. If you click **Clear**, a message asks whether you are sure you want to delete this information. Click **OK** to proceed or **Cancel** to cancel the operation.

**Note:** For help changing the format of the log, see *Log Format Directives in the information area* or on page 79.

Figure 8-7. HTTP Configuration Page

LANTRONIX®

**EDS32PR**  
 Powered by Evolution OS

---

Status

Statistics
Configuration
Authentication
RSS

### HTTP Configuration

HTTP Server:  On  Off

HTTP Port:

HTTPS Port:

Max Timeout:  seconds

Max Bytes:

Logging:  On  Off

Max Log Entries:

Log Format:

Both the **HTTP Port** and **HTTPS Port** (SSL) can be overridden. The HTTP Server will only listen on the **HTTPS Port** when an **SSL Certificate** is configured for the device.

The **Max Timeout** value specifies the maximum amount of time to wait for a request from a client. The **Max Bytes** value specifies the maximum number of bytes allowed in a client request. Both of these value are used to help prevent Denial of Service (DoS) attacks against the HTTP Server.

The HTTP Log is a scrolling log in that only the last **Max Log Entries** lines are cached and viewable.

**Log Format Directives**

- %a remote IP address (could be a proxy)
- %b bytes sent excluding headers
- %B bytes sent excluding headers (0 = '-')
- %h remote host (same as '%a')
- %(h) header contents from request (h = header string)
- %m request method
- %p ephemeral local port value used for request
- %q query string (prepend with '?' or empty '-')
- timestamp HH:MM:SS (same as Apache '%(H:%M:%S)' or '%(T)')
- %u remote user (could be bogus for 401 status)
- %U URL path info
- %r first line of request (same as '%m %U%q <version>')
- %s return status

The max length for each directive is 64 bytes. The exception is '%r' where each element is limited to 64 bytes (i.e. method, URL path info, and query string).

The default log format string is:  
 %h %t "%r" %s %B "%(Referer)" "%(User-Agent)"

---

Network

### Current Configuration

HTTP Status:	On (running)
HTTP Port:	80
HTTPS Port:	443
Max Timeout:	10seconds
Max Bytes:	40960
Logging:	On
Max Log Entries:	50
Log Format:	%h %t "%r" %s %B "%(Referer)" "%(User-Agent)" [Delete]
Logs:	50 entries (8075 bytes)[View] [Clear]

Copyright © Lantronix, Inc. 2005. All rights reserved.

## HTTP Configuration Page

HTTP Configuration Page Settings	Description
HTTP Server	Select whether the HTTP server is enabled. Choices are: <b>On</b> = HTTP server is enabled. ( <i>default</i> ) <b>Off</b> = HTTP server is disabled.
HTTP Port	Enter the number of the port on which the EDS listens for incoming HTTP connections from a Web browser. Default is 80.
HTTPS Port	Enter the number of the port on which the EDS listens for incoming HTTPS connections from a Web browser. Default is 443. The EDS listens on the HTTPS port only when an SSL certificate has been configured for the device (see <a href="#">SSL</a> on page 92).
Max Timeout	Enter the maximum number of seconds that the EDS waits for a request from a client. This value helps prevent Denial of Service (DoS) attacks against the HTTP Server. Default is 10 seconds.
Max Bytes	Enter the maximum number of bytes allowed in a client request. This value helps prevent Denial of Service (DoS) attacks against the HTTP Server. Default is 40960 bytes.
Logging	Select whether the HTTP log is enabled. Choices are: <b>On</b> = HTTP log is enabled. ( <i>default</i> ) <b>Off</b> = HTTP log is disabled.
Max Log Entries	Enter the maximum number of entries that can be cached and viewed in the HTTP log. The HTTP log is a scrolling log, with only the last Max Log Entries cached and viewable. Default is 50.

HTTP Configuration Page Settings	Description
Log Format	<p>Enter the format of the HTTP log. The log format directives are as follows:</p> <ul style="list-style-type: none"> <li>%a remote IP address (could be a proxy)</li> <li>%b bytes sent excluding headers</li> <li>%B bytes sent excluding headers (0 = '-')</li> <li>%h remote host (same as '%a')</li> <li>%{h}i header contents from request (h = header string)</li> <li>%m request method</li> <li>%p ephemeral local port value used for request</li> <li>%q query string (prepend with '?' or empty '-')</li> <li>%t timestamp HH:MM:SS (same as Apache '%(%H:%M:%S)t' or '%(%T)t')</li> <li>%u remote user (could be bogus for 401 status)</li> <li>%U URL path info</li> <li>%r first line of request (same as '%m %U%q &lt;version&gt;')</li> <li>%s return status</li> </ul> <p>The maximum length for each directive is 64 bytes. The exception is '%r' where each element is limited to 64 bytes (i.e. method, URL path info, and query string). The default log format string is: %h %t "%r" %s %B "%{Referer}i" "%{User-Agent}i"</p>

## HTTP Authentication Page

HTTP Authentication allows you to require usernames and passwords to access specific web pages or directories on the EDS's built-in web server.

For example, to add web pages to the EDS to control or monitor of a device attached to a port on the EDS, you can specify the user and password that can access that web page.

If you click **Authentication** at the top of one of the HTTP pages, the HTTP Authentication page displays. Here you can change HTTP authentication settings.

Under **Current Configuration**, **URI** and **Users** have a **Delete** link. If you click **Delete**, a message asks whether you are sure you want to delete this information. Click **OK** to proceed or **Cancel** to cancel the operation.

### Example:

The following example shows how to add authentication to user-loaded web pages in a directory called *port1control*.

1. Create a directory called *port1control* in the EDS's files system (using an FTP client, Windows Explorer, or the EDS Web Manager).
2. Copy the custom web pages to this directory.

3. On the HTTP Authentication page of the EDS Web Manager, add:
  - ◆ A **URI** of port1control
  - ◆ A **Realm** of Monitor
  - ◆ An **AuthType** of Digest
  - ◆ A **Username** and **Password**
4. Click the **Submit** button. The EDS creates a username and password to allow the user to access all web pages located in the directory *port1control* in the EDS file system.

**Note:** The *URI*, *realm*, *username*, and *password* are user-specified, freeform fields. The *URI* must match the directory created on the EDS file system. The *URI* and *realm* used in the example above are only examples and would typically be different as specified by the user.

Figure 8-8. HTTP Authentication Page

LANTRONIX®

EDS32PR

Powered by Evolution OS

Status 🏠

Network

Line

Tunnel

DNS

SNMP

FTP

TFTP

Syslog

HTTP

CLI

Email

SSH

SSL

XML

Filesystem

Protocol Stack

IP Address Filter

Query Port

Diagnostics

System

Statistics
Configuration
Authentication
RSS

## HTTP Authentication

URI:

Realm:

AuthType:  None  Basic  Digest  
 SSL  SSL/Basic  SSL/Digest

Username:

Password:

---

### Current Configuration

URI:	/ [Delete]
Realm:	config
AuthType:	Digest
Users:	admin [Delete]

The HTTP Server can be configured with many different authentication directives. The authentication is hierarchical in that any URI can be given an authentication directive in order to override a parent URI authentication directive.

The different **AuthType** values offer various levels of security. From the least to most secure:

**None**  
no authentication necessary

**Basic**  
encodes passwords using Base64

**Digest**  
encodes passwords using MD5

**SSL**  
page can only be accessed over SSL (no password)

**SSL/Basic**  
page can only be accessed over SSL (encodes passwords using Base64)

**SSL/Digest**  
page can only be accessed over SSL (encodes passwords using MD5)

Note that **SSL** by itself does not require a password but all data transferred to and from the HTTP Server is encrypted.

There is no real reason to create an authentication directive using **None** unless you want to override a parent directive that uses some other **AuthType**.

Multiple users can be configured within a single authentication directive.

Copyright © Lantronix, Inc. 2005. All rights reserved.



## HTTP Authentication Page

HTTP Authentication Page Settings	Description
URI	Enter the Uniform Resource Identifier (URI) of the resource that will participate in the authentication process. Default is /.
Realm	Enter the domain, or realm, used for HTTP operations. Default is <config>.
AuthType	<p>Select an authorization type. Different types of authorization offer varying levels of security. Choices are (from least to most secure):</p> <p><b>None</b> = no authentication necessary.</p> <p><b>Basic</b> = encodes passwords using Base64.</p> <p><b>Digest</b> = encodes passwords using MD5. (Default)</p> <p><b>SSL</b> = page can only be accessed over SSL (no password).</p> <p><b>SSL/Basic</b> = page can only be accessed over SSL (encodes passwords using Base64).</p> <p><b>SSL/Digest</b> = page can only be accessed over SSL (encodes passwords using MD5).</p> <p>SSL alone does not require a password, but all data transferred to and from the HTTP Server is encrypted. There is no reason to create an authentication directive using None, unless you want to override a parent directive that uses some other AuthType. Multiple users can be configured within a single authentication directive.</p>
Username	Enter the name of the user who will participate in the authentication. Default is admin.
Password	Enter the password that will be associated with the username. Default is PASS.

## HTTP RSS Page

If you click **RSS** at the top of one of the HTTP pages, the HTTP RSS page displays. Here you can specify RDF Site Summary (RSS) information. RSS is a way of feeding online content to Web users. Instead of actively searching for EDS configuration changes, RSS feeds allow viewing of only relevant and new information regarding changes made to the EDS via an RSS publisher.

Under **Current Configuration**, Data has **View** and **Clear** links. If you click **View**, the data displays. If you click **Clear**, a message asks whether you are sure you want to delete this information. Click **OK** to proceed or **Cancel** to cancel the operation.

Figure 8-9. HTTP RSS Page

The screenshot shows the LANTRONIX EDS configuration interface. The top header includes the LANTRONIX logo and 'EDS Powered by Evolution OS'. A navigation bar contains 'Statistics', 'Configuration', 'Authentication', and 'RSS'. The left sidebar lists various system categories like Network, Line, Tunnel, DNS, etc. The main content area is titled 'HTTP RSS' and contains the following settings:

- RSS Feed:  On  Off
- Persistent:  On  Off
- Max Entries:
- Submit button

Below these settings is a 'Current Configuration' table:

RSS Feed:	Off
Persistent:	Off
Max Entries:	100
Data:	0 entries (0 bytes) <a href="#">View</a> <a href="#">Clear</a>

On the right side of the page, there is explanatory text about RSS feeds, including details about the file used for configuration changes and the timestamp format for each entry.

Copyright © Lantronix, Inc. 2005. All rights reserved.

## HTTP RSS Page

HTTP RSS Page Settings	Description
RSS Feed	<p>Select whether an RSS feed is enabled or disabled. An RSS syndication feed is served by the HTTP server. This feed contains up-to-date information about configuration changes that occur on the EDS. Choices are:</p> <p><b>On</b> = RSS feed is enabled.</p> <p><b>Off</b> = RSS feed is disabled. (<i>default</i>)</p>
Persistent	<p>Select whether the RSS feed is persistent. Choices are:</p> <p><b>On</b> = data is stored on the filesystem, in the file "/cfg_log.txt." This allows feed data to be available across reboots or until the factory defaults are set.</p> <p><b>Off</b> = data is not stored on the filesystem. (<i>default</i>)</p>
Max Entries	<p>Enter the maximum number of log entries. The RSS feed is a scrolling feed, with only the last <b>Max Entries</b> entries cached and viewable. To be notified automatically about any configuration changes that occur, register the RSS feed within your favorite RSS aggregator. Default is 100.</p> <p>Each RSS feed entry is prefixed with a timestamp "[BC:HH:MM:SS]". BC is the Boot Cycle value and indicates the number of times the EDS has rebooted since factory defaults were last loaded. The resulting "HH:MM:SS" is the time since the EDS booted.</p>

## 9: Security Settings

### SSH Pages

Clicking the **SSH** link in the menu bar displays the SSH Server: Host Keys page. This page has four links at the top for viewing and changing SSH server host keys, SSH server authorized keys, SSH client known hosts, and SSH client users.

*Note:* For more information, see [SSH](#) on page 143.

#### SSH Server: Host Keys Page

The SSH Server: Host Keys page displays when you click **SSH** in the menu bar. It also displays when you click **SSH Server: Host Keys** at the top of one of the other SSH pages. Here you can create new keys and upload them to an SSH server.

SSH server private and public host keys are used by all applications that play the role of an SSH server, specifically the CLI and tunneling in Accept mode. These keys can be created elsewhere and uploaded to the device, or automatically generated on the device.

Under **Current Configuration**, **Public RSA Key** and **Public DSA Key** have **View** and **Delete** links if these keys have been created. If you click **View**, the key displays. If you click **Delete**, a message asks whether you are sure you want to delete this information. Click **OK** to proceed or **Cancel** to cancel the operation.

Figure 9-1. SSH Server: Host Keys Page

LANTRONIX®
EDS32PR  
Powered by Evolution OS

Status

Network

Line

Tunnel

DNS

SNMP

FTP

TFTP

Syslog

HTTP

CLI

Email

SSH

SSL

XML

Filesystem

Protocol Stack

IP Address Filter

Query Port

Diagnostics

RTC

System

SSH Server: Host Keys    SSH Client: Known Hosts  
SSH Server: Authorized Users    SSH Client: Users

## SSH Server: Host Keys

### Upload Keys

Private Key:

Public Key:

Key Type:     RSA     DSA

### Create New Keys

Key Type:     RSA     DSA

Bit Size:     512     768     1024

---

### Current Configuration

Public RSA Key:	<a href="#">[View Key]</a> <a href="#">[Delete Key]</a>
Public DSA Key:	<a href="#">[View Key]</a> <a href="#">[Delete Key]</a>

The SSH Server Host Keys are used by all applications that play the role of an SSH Server. Specifically the Command Line Interface (CLI) and Tunneling in Accept Mode. These keys can be created elsewhere and uploaded to the device or automatically generated on the device.

If uploading existing keys, take care to ensure the Private Key will not be compromised in transit. This implies the data is uploaded over some kind of secure private network.

WARNING: When generating new keys, using a larger **Bit Size** will result in a longer key generation time. Tests on this hardware have shown it can take upwards of:

- 10 seconds for a 512 bit RSA Key
- 1 minute for a 768 bit RSA Key
- 2 minutes for a 1024 bit RSA Key
- 2 minutes for a 512 bit DSA Key
- 10 minutes for a 768 bit DSA Key
- 15 minutes for a 1024 bit DSA Key

Note that some SSH Clients require RSA Host Keys to be at least 1024 bits in size.

Copyright © Lantronix, Inc. 2005. All rights reserved.

## SSH Server: Host Keys Page

SSH Server: Host Keys Page Settings	Description
<b>Upload Keys</b>	
Private Key	Enter the path and name of the existing private key you want to upload or use the <b>Browse</b> button to select the key. Be sure the private key will not be compromised in transit. This implies the data is uploaded over some kind of secure private network.
Public Key	Enter the path and name of the existing public key you want to upload or use the <b>Browse</b> button to select the key.
Key Type	Select a key type to be used. Choices are: <b>RSA</b> = use this key with SSH1 and SSH2 protocols. <b>DSA</b> = use this key with the SSH2 protocol.
<b>Create New Keys</b>	
Key Type	Select a key type to be used for the new key. Choices are: <b>RSA</b> = use this key with the SSH1 and SSH2 protocols. <b>DSA</b> = use this key with the SSH2 protocol.
Bit Size	Select a bit length for the new key. Choices are: <b>512</b> <b>768</b> <b>1024</b> Using a larger bit size takes more time to generate the key. Approximate times are: 10 seconds for a 512-bit RSA key 1 minute for a 768-bit RSA key 2 minutes for a 1024-bit RSA key 2 minutes for a 512-bit DSA key 10 minutes for a 768-bit DSA key 15 minutes for a 1024-bit DSA key Some SSH clients require RSA host keys to be at least 1024 bits long.

## SSH Client: Known Hosts Page

If you click **SSH Client: Known Hosts** at the top of one of the SSH pages, the SSH Client: Known Hosts page displays. Here you can change SSH client settings for known hosts.

**Note:** You do not have to complete the fields on this page for communication to occur. However, completing them adds another layer of security that protects against Man-In-The-Middle (MITM) attacks.

Figure 9-2. SSH Client: Known Hosts Page

SSH Client: Known Hosts Page

SSH Client: Known Hosts Page Settings	Description
Server	Enter the name or IP address of a known host. If you entered a server name, the name should match the name of the server used as the <b>Remote Address</b> in Connect mode tunneling.
Public RSA Key	Enter the path and name of the existing public RSA key you want to use with this known host or use the <b>Browse</b> button to select the key.
Public DSA Key	Enter the path and name of the existing public DSA key you want to use with this known host or use the <b>Browse</b> button to select the key.

## SSH Server: Authorized Users Page

If you click **SSH Server: Authorized Users** at the top of one of the SSH pages, the SSH Server: Authorized Users page displays. Here you can change SSH server settings for authorized users.

SSH Server Authorized Users are accounts on the EDS that can be used to log into the EDS via SSH. For instance, these accounts can be used to SSH into the CLI or open an SSH connection to a device port. Every account must have a password.

The user's public keys are optional and only necessary if public key authentication is wanted. Using public key authentication allows a connection to be made without the password being asked.

Under **Current Configuration**, **User** has a **Delete User** link, and **Public RSA Key** and **Public DSA Key** have **View Key** and **Delete Key** links. If you click a **Delete** link, a message asks whether you are sure you want to delete this information. Click **OK** to proceed or **Cancel** to cancel the operation.

Figure 9-3. SSH Server: Authorized Users Page

The screenshot displays the LANTRONIX EDS32PR web interface. The top header includes the LANTRONIX logo and 'EDS32PR Powered by Evolution OS'. A left-hand navigation menu lists various system settings like Network, Line, Tunnel, DNS, etc. The main content area is titled 'SSH Server: Authorized Users' and contains several input fields: Username, Password, Public RSA Key (with a 'Browse...' button), and Public DSA Key (with a 'Browse...' button). Below these fields is an 'Add/Edit' button. A 'Current Configuration' section shows a table with the following data:

User:	gary [Delete User]
Password:	Configured
Public RSA Key:	[View Key] [Delete Key]
Public DSA Key:	[View Key] [Delete Key]

On the right side, a sidebar provides additional information: 'The SSH Server Authorized Users are used by all applications that play the role of an SSH Server. Specifically the Command Line Interface (CLI) and Tunneling in Accept Mode. Every user account must have a Password. The user's Public Keys are optional and only necessary if public key authentication is wanted. Using public key authentication will allow a connection to be made without the password being asked.'

Copyright © Lantronix, Inc. 2005. All rights reserved.



## SSH Server: Authorized Users Page

SSH Server: Authorized Users Page Settings	Description
Username	Enter the name of the user authorized to access the SSH server.
Password	Enter the password associated with the username.
Public RSA Key	Enter the path and name of the existing public RSA key you want to use with this user or use the <b>Browse</b> button to select the key. If authentication is successful with the key, no password is required.
Public DSA Key	Enter the path and name of the existing public DSA key you want to use with this user or use the <b>Browse</b> button to select the key. If authentication is successful with the key, no password is required.

## SSH Client: Users Page

If you click **SSH Client: Users** at the top of one of the SSH pages, the SSH Client: Users page displays. Here you can change SSH client settings for users.

SSH client known hosts are used by all applications that play the role of an SSH client, specifically tunneling in Connect mode. At the very least, a password or key pair must be configured for a user. The keys for public key authentication can be created elsewhere and uploaded to the device or automatically generated on the device. If uploading existing keys, be sure the private key will not be compromised in transit. This implies the data is uploaded over some kind of secure private network.

**Note:** If you are providing a key by uploading a file, make sure that the key is not password protected.

Figure 9-4. SSH Client: Users Page

LANTRONIX®

EDS32PR

Powered by Evolution OS

---

Status

Network

Line

Tunnel

DNS

SNMP

FTP

TFTP

Syslog

HTTP

CLI

Email

SSH

SSL

XML

Filesystem

Protocol Stack

IP Address Filter

Query Port

Diagnostics

System

SSH Server: Host Keys
SSH Client: Known Hosts

SSH Server: Authorized Users
SSH Client: Users

## SSH Client: Users

Username:

Password:

Remote Command:

Private Key:

Public Key:

Key Type:  RSA  DSA

### Create New Keys

Note: User must first be created using the form above.

Username:

Key Type:  RSA  DSA

Bit Size:  512  768  1024

---

### Current Configuration

User:	gary <a href="#">[Delete User]</a>
Password:	Configured
Remote Command:	shell
Public RSA Key:	No RSA Key Configured
Public DSA Key:	No DSA Key Configured

User:	tester <a href="#">[Delete User]</a>
Password:	Configured
Remote Command:	shell
Public RSA Key:	No RSA Key Configured
Public DSA Key:	No DSA Key Configured

The SSH Client Known Hosts are used by all applications that play the role of an SSH Client. Specifically Tunneling in Connect Mode.

At the very least, a **Password** or **Key Pair** must be configured for a user. The keys for public key authentication can be created elsewhere and uploaded to the device or automatically generated on the device.

If uploading existing Keys, take care to ensure the Private Key will not be compromised in transit. This implies the data is uploaded over some kind of secure private network.

WARNING: When generating new Keys, using a larger **Bit Size** will result in a longer key generation time. Tests on this hardware have shown it can take upwards of:

- 10 seconds for a 512 bit RSA Key
- 1 minute for a 768 bit RSA Key
- 2 minutes for a 1024 bit RSA key
- 2 minutes for a 512 bit DSA Key
- 10 minutes for a 768 bit DSA Key
- 15 minutes for a 1024 bit DSA key

The default **Remote Command** is 'shell' which tells the SSH Server to execute a remote shell upon connection. This command can be changed to anything the SSH Server on the remote host can execute.

Copyright © Lantronix, Inc. 2005. All rights reserved.

## SSH Client: Users Page

SSH Client: Users Page Settings	Description
Username	Enter the name that the EDS uses to connect to the SSH client user.
Password	Enter the password associated with the username.
Remote Command	Enter the command that can be executed remotely. Default is "shell," which tells the SSH server to execute a remote shell upon connection. This command can be changed to anything the remote host can perform.
Private Key	Enter the name of the existing private key you want to use with this SSH client user. You can either enter the path and name of the key, or use the <b>Browse</b> button to select the key.
Public Key	Enter the path and name of the existing public key you want to use with this SSH client user or use the <b>Browse</b> button to select the key.
Key Type	Select the key type to be used. Choices are: <b>RSA</b> = use this key with the SSH1 and SSH2 protocols. <b>DSA</b> = use this key with the SSH2 protocol.
<b>Create New Keys</b>	
Username	Enter the name of the user associated with the new key.
Key Type	Select the key type to be used for the new key. Choices are: <b>RSA</b> = use this key with the SSH1 and SSH2 protocols. <b>DSA</b> = use this key with the SSH2 protocol.
Bit Size	Select the bit length of the new key. Choices are: <b>512</b> <b>768</b> <b>1024</b> Using a larger Bit Size takes more time to generate the key. Approximate times are: 10 seconds for a 512-bit RSA key 1 minute for a 768-bit RSA key 2 minutes for a 1024-bit RSA key 2 minutes for a 512-bit DSA key 10 minutes for a 768-bit DSA key 15 minutes for a 1024-bit DSA key Some SSH clients require RSA host keys to be at least 1024 bits long.

## SSL Page

Clicking the **SSL** link in the menu bar displays the SSL page. Here you can upload an existing SSL certificate or create a new self-signed one.

**Note:** For more information about SSL, see [SSL on page 141](#).

An SSL certificate must be configured for the HTTP server to listen on the HTTPS port. This certificate can be created elsewhere and uploaded to the device or automatically generated on the device. A certificate generated on the device will be self-signed. If uploading an existing SSL certificate, be sure the private key will not be compromised in transit. This implies the data is uploaded over some kind of secure private network.

At the bottom of this page is the current SSL certificate, if any. Under **Current SSL Certificate**, there is a **Delete** link. If you click **Delete**, a message asks whether you are sure you want to delete the current certificate. Click **OK** to proceed or **Cancel** to cancel the operation.

Figure 9-5. SSL Page

**LANTRONIX**<sup>®</sup>
**EDS32PR**  
Powered by **Evolution OS**

- Status
- Network**
- Line
- Tunnel
- DNS
- SNMP
- FTP
- TFTP
- Syslog
- HTTP
- CLI
- Email
- SSH
- SSL
- XML
- Filesystem
- Protocol Stack
- IP Address Filter
- Query Port
- Diagnostics
- RTC
- System

## SSL

### Upload Certificate

New Certificate:

New Private Key:

### Create New Self-Signed Certificate

Country (2 Letter Code):

State/Province:

Locality (City):

Organization:

Organization Unit:

Common Name:

Expires:  mm/dd/yyyy

Bit Size:  512  768  1024



---

### Current SSL Certificate

The SSL Certificate has been generated.  
The HTTP Server has been restarted.

[Delete]

<b>Version:</b>	3 (0x02)
<b>Serial Number:</b>	00
<b>Signature Algorithm:</b>	md5WithRSAEncryption
<b>Issuer:</b>	C: US ST: CA L: IRV O: WIDGETS INC OU: ENG CN: www.widgets.com
<b>Validity:</b>	<b>Issued On:</b> Jan 01 00:00:00 2005 GMT <b>Expires On:</b> Jan 01 00:00:00 2010 GMT
<b>Subject:</b>	C: US ST: CA L: IRV O: WIDGETS INC OU: ENG CN: www.widgets.com
<b>Subject Public Key:</b>	512-bit d0 fc e2 71 cc d2 63 49 02 9c 88 8d a4 4b 13 5d 39 7a 42 f9 ef 41 32 bd 7c 7c 14 a4 f6 19 52 39 49 46 ef fb 86 dc 1b af 4d fe c8 fa 12 3f 99 1e 6f 40 d2 66 af c2 1d 7b 4c 0e 3e 8b 21 f7 3b 5f

An SSL Certificate must be configured in order for the HTTP Server to listen on the HTTPS Port. This certificate can be created elsewhere and uploaded to the device or automatically generated on the device. A certificate generated on the device will be self-signed.

If uploading an existing SSL Certificate, take care to ensure the Private Key will not be compromised in transit. This implies the data is uploaded over some kind of secure private network.

WARNING: When generating a new self-signed SSL Certificate, using a larger **Bit Size** will result in a longer key generation time. Tests on this hardware have shown it can take upwards of:

- 10 seconds for a 512 bit RSA Key
- 1 minute for a 768 bit RSA Key
- 2 minutes for a 1024 bit RSA Key

Copyright © Lantronix, Inc. 2005. All rights reserved.

## SSL Page

SSL Page Settings	Description
<b>Upload Certificate</b>	
New Certificate	Enter the path and name of the existing certificate you want to upload, or use the <b>Browse</b> button to select the certificate.
New Private Key	Enter the path and name of the existing private key you want to upload, or use the <b>Browse</b> button to select the private key.
<b>Create New Self-Signed Certificate</b>	
Country (2 Letter Code)	Enter the 2-letter country code to be assigned to the new self-signed certificate.  Examples: US for United States and CA for Canada
State/Province	Enter the state or province to be assigned to the new self-signed certificate.
Locality (City)	Enter the city or locality to be assigned to the new self-signed certificate.
Organization	Enter the organization to be associated with the new self-signed certificate.  <b>Example:</b> If your company is called Widgets, and you are setting up a Web server for the Sales department, enter Widgets for the Organization.
Organization Unit	Enter the organizational unit to be associated with the new self-signed certificate.  <b>Example:</b> If your company is setting up a Web server for the Sales department, enter Sales for your Organizational Unit.
Common Name	Enter the same name that the user will enter when requesting your Web site.  <b>Example:</b> If a user enters http://www.widgets.abccompany.com to access your Web site, the <b>Common Name</b> would be www.widgets.abccompany.com.
Expires	Enter the expiration date, in mm/dd/yyyy format, for the new self-signed certificate.  <b>Example:</b> An expiration date of May 9, 2007 is entered as 05/05/2007.
Bit Size	Select the bit size of the new self-signed certificate. Choices are:  <b>512</b> <b>768</b> <b>1024</b>  Using a larger bit size takes more time to generate the key. Approximate times are:  10 seconds for a 512-bit RSA key  1 minute for a 768-bit RSA key  2 minutes for a 1024-bit RSA key

# 10: Maintenance and Diagnostics Settings

## Filesystem Pages

Clicking the **Filesystem** link in the menu bar displays the Filesystem Statistics page. This page has two links at the top for viewing filesystem statistics and browsing and manipulating the entire filesystem.

### Filesystem Statistics Page

The Filesystem Statistics page displays when you click **Filesystem** in the menu bar. It also displays when you click **Statistics** at the top of the Filesystem Browser page. This page displays various statistics and current usage information of the flash filesystem.

The **Actions** row provides **Compact** and **Format** links for compacting or formatting the filesystem. Only a system administrator should perform these tasks.

**Note:** *Compact preserves data and eliminates dirty space by making a new copy. Format destroys all of the data in the filesystem.*

Figure 10-1. Filesystem Statistics Page

The screenshot shows the Lantronix EDS32PR web interface. The top header includes the Lantronix logo and 'EDS32PR Powered by Evolution OS'. A left-hand navigation menu lists various system settings, with 'Filesystem' highlighted. The main content area is titled 'Filesystem Statistics' and contains a table of statistics and two buttons: 'Compact' and 'Format'. A note on the right side of the page states: 'This page displays various statistics and current usage information of the flash filesystem. The filesystem can be compacted or formatted here. Make sure you know what you're doing before formatting the filesystem.'

Filesystem Size:	2.625000 Mbytes (2752512 bytes)
Available Space:	1.533184 Mbytes (1607661 bytes) (58%)
Clean Space:	784.409 Kbytes (803235 bytes) (29%)
Dirty Space:	785.572 Kbytes (804426 bytes) (29%)
File & Dir Space Used:	1.091814 Mbytes (1144851 bytes) (41%)
Data Space Used:	1.081322 Mbytes (1133849 bytes)
Number of Files:	156
Number of Dirs:	2
Number of System Files:	0
Opened Files:	0
Locked Files:	0
Opened for Sharing:	0
Current Bank:	A
FW Sectors:	00 - 21, 18 erase cycles
Bank A Sectors:	22 - 43, 6 erase cycles
Bank B Sectors:	43 - 64, 5 erase cycles
Busy:	No
Actions:	[Compact] [Format]

## Filesystem Browser Page

If you click **Browse** at the top of a Filesystem page, the Filesystem Browser page displays. Here you can browse and manipulate the entire filesystem. For example, you can:

- ◆ Browse the filesystem.
- ◆ Create files and directories.
- ◆ Upload files via HTTP.
- ◆ Copy and move files.
- ◆ Transfer files to and from a TFTP server.

Figure 10-2. Filesystem Browser Page

The screenshot shows the Filesystem Browser page for the EDS32PR device. The interface includes a sidebar with navigation options (Status, Network, Line, Tunnel, DNS, SNMP, FTP, TFTP, Syslog, HTTP, CLI, Email, SSH, SSL, XML, Filesystem, Protocol Stack, IP Address Filter, Query Port, Diagnostics, System) and a main content area. The main content area has a top navigation bar with 'Statistics' and 'Browse' buttons. Below this, the 'Filesystem Browser' section displays a directory listing for the root directory (/) with two files: 'http' and 'Config-2-days-testing.xml', both 248,468 Kbytes (254,432 bytes). The 'Create' section has input fields for 'File:' and 'Directory:' with 'Create' buttons. The 'Upload File' section has a 'Browse...' button and an 'Upload' button. The 'Copy File' section has 'Source:' and 'Destination:' input fields and a 'Copy' button. The 'Move' section has 'Source:' and 'Destination:' input fields and a 'Move' button. The 'TFTP' section has radio buttons for 'Action:' (Get, Put) and 'Mode:' (ASCII, Binary), and input fields for 'Local File:', 'Remote File:', 'Host:', and 'Port:', with a 'Transfer' button. A footer note states: 'Copyright © Lantronix, Inc., 2005. All rights reserved.'



## Filesystem Browser Page

Filesystem Browser Page Settings	Description
<b>Create</b>	
File	Enter the name of the file you want to create, and then click <b>Create</b> .
Directory	Enter the name of the directory you want to create, and then click <b>Create</b> .
<b>Upload File</b>	Enter the path and name of the file you want to upload via HTTP or use the <b>Browse</b> button to select the file, and then click <b>Upload</b> .
<b>Copy File</b>	
Source	Enter the location where the file you want to copy resides.
Destination	Enter the location where you want the file copied. After you specify a source and destination, click <b>Copy</b> to copy the file.
<b>Move</b>	
Source	Enter the location where the file you want to move resides.
Destination	Enter the location where you want the file moved. After you specify a source and destination, click <b>Move</b> to move the file.
<b>TFTP</b>	
Action	Select the action that is to be performed via TFTP. Choices are:  <b>Get</b> = a “get” command will be executed to store a file locally.  <b>Put</b> = a “put” command will be executed to send a file to a remote location.
Mode	Select a TFTP mode to use. Choices are:  <b>ASCII</b>  <b>Binary</b>
Local File	Enter the name of the local file on which the specified “get” or “put” action is to be performed.
Remote File	Enter the name of the file at the remote location that is to be stored locally (“get”) or externally (“put”).
Host	Enter the IP address or name of the host involved in this operation.
Port	Enter the number of the port involved in TFTP operations. Click <b>Transfer</b> to complete the TFTP transfer.

## Diagnostics Pages

The EDS has several tools for performing diagnostics. To view these diagnostic tools, click the **Diagnostics** link in the menu bar to display the Diagnostics: Hardware page. The available diagnostic tools appear at the top of the page.

### Diagnostics: Hardware Page

The Diagnostics: Hardware page displays when you click **Diagnostics** in the menu bar. It also displays when you click **Hardware** at the top of one of the other Diagnostic pages. This read-only page displays the current hardware configuration.

The screenshot shows the Lantronix EDS32PR web interface. The top bar includes the Lantronix logo and 'EDS32PR Powered by Evolution OS'. A left-hand navigation menu lists various system pages, with 'Diagnostics' highlighted. The main content area is titled 'Diagnostics: Hardware' and 'Current Configuration'. It features a sub-menu with 'Hardware' selected, and a table of hardware specifications.

Diagnostics: Hardware	
Current Configuration	
CPU Type:	IXP420
CPU Speed:	266.0 MHz
CPU Instruction Cache:	32.000 Kbytes (32768 bytes)
CPU Data Cache:	32.000 Kbytes (32768 bytes)
RAM Size:	16.000000 Mbytes (16777216 bytes)
Flash Size:	8.000000 Mbytes (8388608 bytes)
Flash Sector Size:	128.000 Kbytes (131072 bytes)
Flash Sector Count:	64
Flash ID:	0xEE11

Copyright © Lantronix, Inc. 2005. All rights reserved.

## MIB-II Network Statistics Page

Clicking **MIB-II Stats** from one of the Diagnostics pages displays the MIB-II Network Statistics page. This page displays the various SNMP-served Management Information Bases (MIBs) available on the EDS. Information about these MIBs can be found in the following Request for Comments (RFCs):

- ◆ RFC 1213, Original MIB-II definitions
- ◆ RFC 2011, Updated definitions for IP and ICMP
- ◆ RFC 2012, Updated definitions for TCP
- ◆ RFC 2013, Updated definitions for UDP
- ◆ RFC 2096, Definitions for IP Forwarding

Figure 10-3. MIB-II Network Statistics Page

The screenshot shows the MIB-II Network Statistics page. At the top, the Lantronix logo and 'EDS32PR Powered by Evolution OS' are visible. A navigation menu on the left lists various system components, with 'Diagnostics' selected. The main content area has a breadcrumb trail: Hardware > MIB-II > IP Sockets > MIB-II Network Statistics. Below this, a list of MIB-II statistics groups is provided as links: System Group, Interface Group, Interface Table, IP Group, IP Address Table, IP Net To Media Table, IP Forward Group, IP Forward Table, ICMP Group, TCP Group, TCP Connection Table, UDP Group, and UDP Table. On the right, a sidebar explains that users can view various SNMP-served MIBs and lists the following RFCs: RFC 1213 (Original MIB-II definitions), RFC 2011 (Updated definitions for IP and ICMP), RFC 2012 (Updated definitions for TCP), RFC 2013 (Updated definitions for UDP), and RFC 2096 (Definitions for IP Forwarding). The footer contains the copyright notice: Copyright © Lantronix, Inc. 2005. All rights reserved.

## IP Sockets Page

Clicking **IP Sockets** from one of the Diagnostics pages displays the IP Sockets page. This read-only page lists all the network sockets on the EDS that are currently open.

Figure 10-4 IP Sockets Page

The screenshot displays the LANTRONIX EDS interface. At the top, the LANTRONIX logo is on the left and 'EDS Powered by Evolution OS' is on the right. A navigation menu on the left lists various system components, with 'IP Sockets' highlighted. The main content area features a sub-navigation bar with 'IP Sockets' selected, and a table titled 'IP Sockets' listing active network connections. A note on the right explains that the page lists all currently open network sockets on the device.

Protocol	RxQ	TxQ	LocalAddr:Port	RemoteAddr:Port	State
TCP	0	0	172.20.198.26:80	255.255.255.255:0	LISTEN
TCP	0	0	172.20.198.26:21	255.255.255.255:0	LISTEN
UDP	0	0	172.20.198.26:69	255.255.255.255:0	
UDP	0	0	172.20.198.26:161	255.255.255.255:0	
UDP	0	0	172.20.198.26:30718	172.20.198.28:28678	ESTABLISHED
TCP	0	0	172.20.198.26:10001	255.255.255.255:0	LISTEN
TCP	0	0	172.20.198.26:10002	255.255.255.255:0	LISTEN
TCP	0	0	172.20.198.26:10003	255.255.255.255:0	LISTEN
TCP	0	0	172.20.198.26:10004	255.255.255.255:0	LISTEN
TCP	0	0	172.20.198.26:23	255.255.255.255:0	LISTEN
TCP	0	0	172.20.198.26:22	255.255.255.255:0	LISTEN
TCP	0	4	172.20.198.26:80	172.18.100.40:2528	ESTABLISHED
TCP	0	0	172.20.198.26:20	172.20.198.28:15182	ESTABLISHED

Copyright © Lantronix, Inc. 2005. All rights reserved.

## Diagnostics: Ping Page

Figure 10-5 Diagnostics: Ping Page

The screenshot shows the Lantronix EDS32PR web interface. The top navigation bar includes the Lantronix logo and 'EDS32PR Powered by Evolution OS'. A left-hand navigation menu lists various system settings. The main content area is titled 'Diagnostics: Ping' and features a 'Ping' button, a 'Host' input field, a 'Count' input field with the value '3', and a 'Timeout' input field with the value '5' and the unit 'seconds'. A 'Submit' button is located below the input fields. To the right of the main content area, there is a help text box that reads: 'Specify either a DNS Hostname or IP Address when pinging a network host. Additionally, the **Count** specifies the number of ping packets to send and the **Timeout** specifies how long to wait for a response for each ping packet sent.'

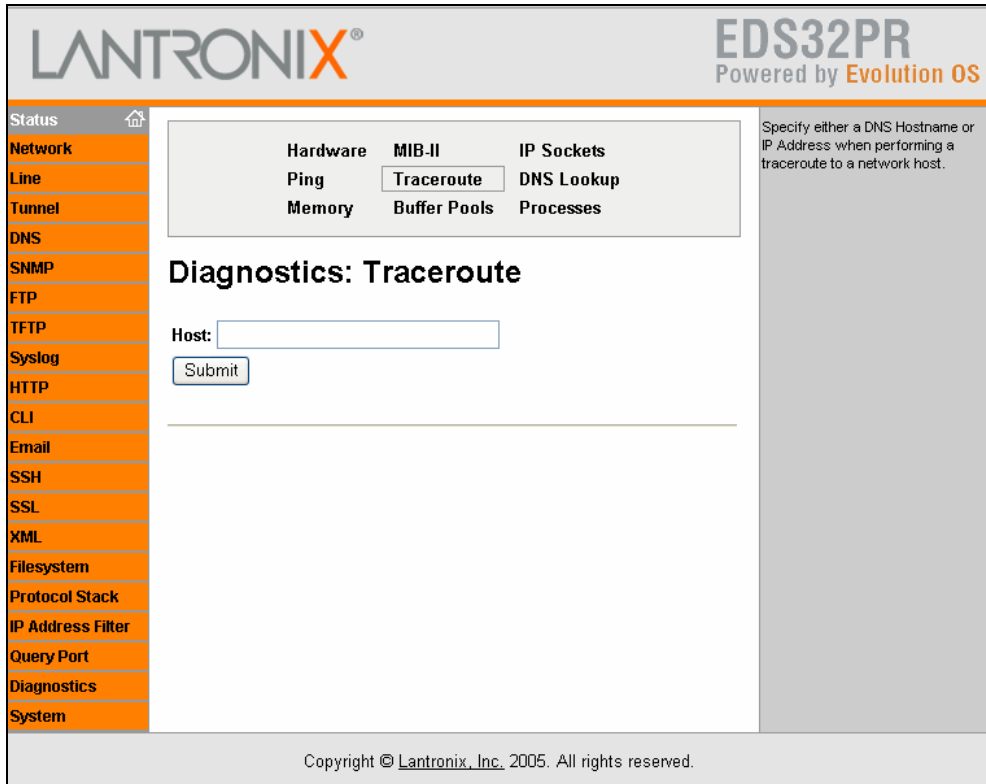
### Diagnostics: Ping Page

Diagnostics: Ping Page Settings	Description
Host	Enter the IP address you want the EDS to ping.
Count	Enter the number of ping packets that the EDS should try to send to the Host. Default is 3.
Timeout	Enter the maximum number of seconds that the EDS should wait for a response from the host before timing out. Default is 5 seconds.

## Diagnostics: Traceroute Page

Clicking **Traceroute** from one of the Diagnostics pages displays the Diagnostics: Traceroute page. Here you can trace a packet from the EDS to an Internet host, showing how many hops the packet requires to reach the host and how long each hop takes. If you visit a Web site whose pages appear slowly, you can use traceroute to determine where the longest delays are occurring.

Figure 10-6 Diagnostics: Traceroute Page



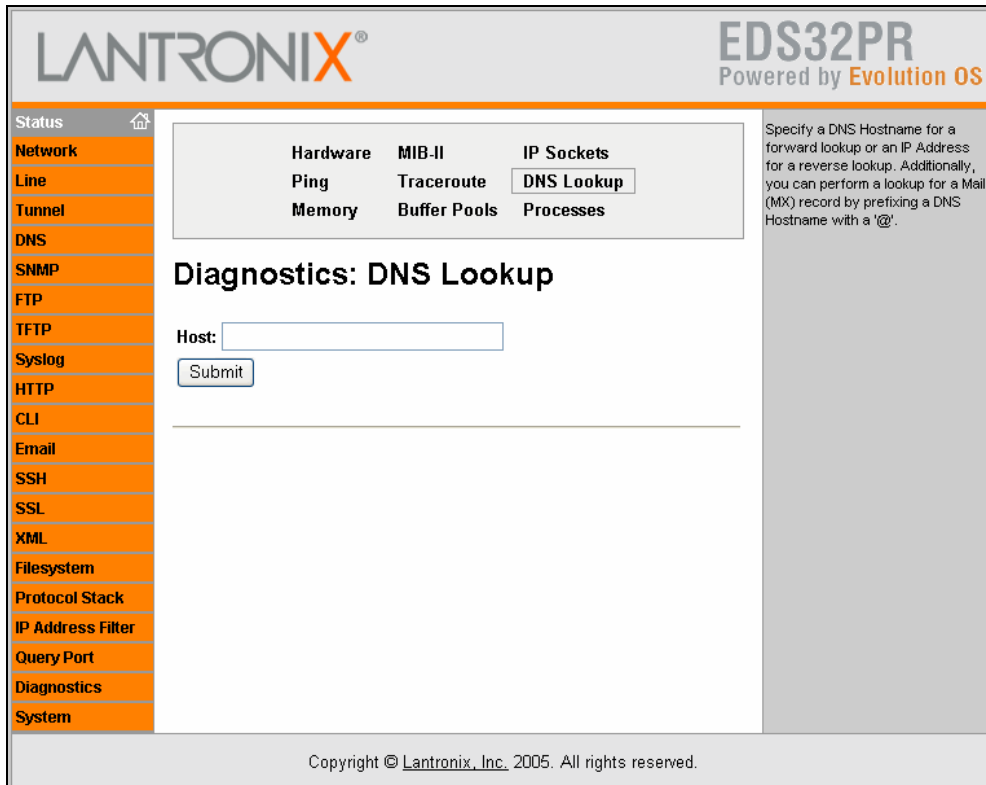
### Diagnostics: Traceroute Page

Diagnostics: Traceroute Page Settings	Description
Host	Enter the IP address or DNS host name of the remote host that you want to traceroute from the EDS.

## Diagnostics: DNS Lookup Page

Clicking **DNS Lookup** from one of the Diagnostics pages displays the Diagnostics: DNS Lookup page. Here you can specify a DNS Hostname for a forward lookup or an IP address for a reverse lookup. You can also perform a lookup for a Mail (MX) record by prefixing a DNS Hostname with a '@'.

Figure 10-7 Diagnostics: DNS Lookup Page



Diagnostics: DNS Lookup Page

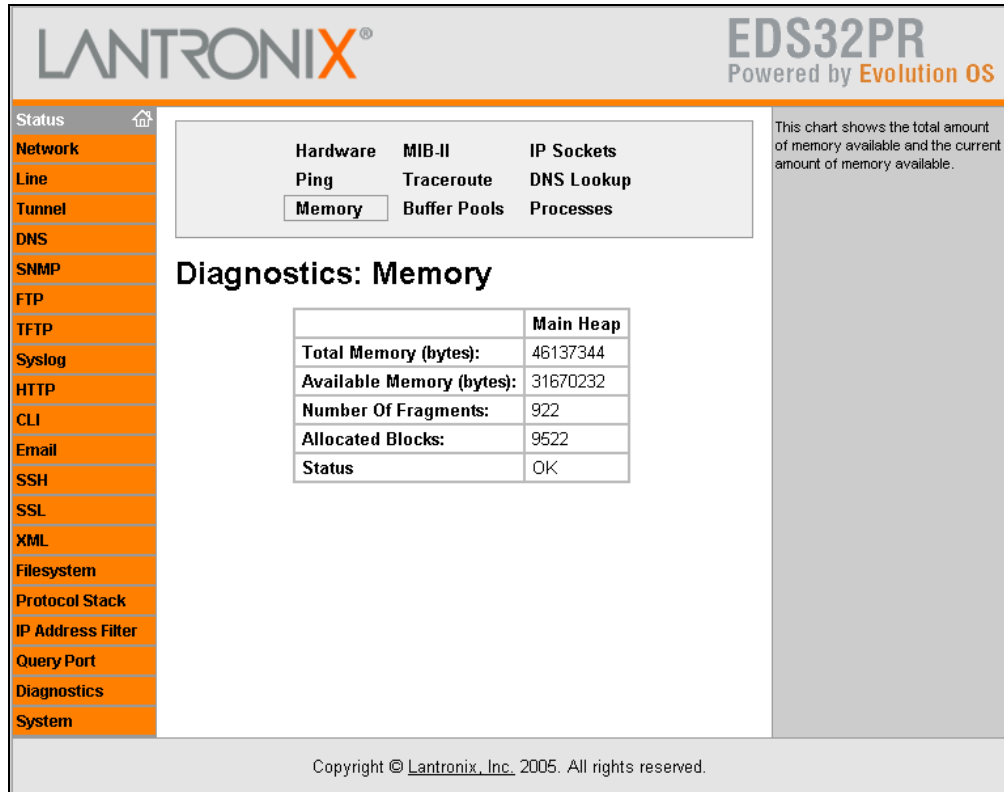
Diagnostics: DNS Lookup Page Settings	Description
Host	<p>Perform one of the following:</p> <p>For reverse lookup to locate the hostname for that IP address, enter an IP address.</p> <p>For forward lookup to locate the corresponding IP address, enter a hostname.</p> <p>To look up the Mail Exchange (MX) record IP address, enter a domain name prefixed with "@".</p>

## Diagnostics: Memory Page

Clicking **Memory** from one of the Diagnostics pages displays the Diagnostics: Memory. This read-only page shows the total memory and available memory (in bytes), along with the number of fragments, allocated blocks, and memory status.

The Diagnostics: Memory page also shows the current amount of available memory.

Figure 10-8 Diagnostics: Memory Page






## Diagnostics: Buffer Pool

Clicking **Buffer Pools** from one of the diagnostics page displays a read-only screen that shows the current usage of the private buffer pools. Private buffer pools are used in various parts of the system to ensure deterministic memory management, thus eliminating any contention for memory from the generic heap space.

Figure 10-9. Diagnostics: Buffer Pools Page



**EDS4100**  
 Powered by **Evolution OS**

Status

**Network**

Line

Tunnel

DNS

SNMP

FTP

TFTP

Syslog

HTTP

CLI

Email

SSH

SSL

XML

Filesystem

Protocol Stack

IP Address Filter

Query Port

**Diagnostics**

System

Hardware MIB-II IP Sockets

Ping Traceroute DNS Lookup

Memory Buffer Pools Processes

### Diagnostics: Buffer pools

Network Stack Buffer Pool				
	Total	Free	Used	MaxUsed
Buffer Headers	512	510	2	12
Cluster Pool Size: 2048	256	253	3	10

Ethernet Driver Buffer Pool				
	Total	Free	Used	MaxUsed
Buffer Headers	2048	1920	128	151
Cluster Pool Size: 2112	1024	896	128	151

Serial Driver Line 1 Buffer Pool				
	Total	Free	Used	MaxUsed
Buffer Headers	256	128	128	128
Cluster Pool Size: 512	128	0	128	128

Serial Driver Line 2 Buffer Pool				
	Total	Free	Used	MaxUsed
Buffer Headers	256	128	128	128
Cluster Pool Size: 512	128	0	128	128

Serial Driver Line 3 Buffer Pool				
	Total	Free	Used	MaxUsed
Buffer Headers	256	128	128	128
Cluster Pool Size: 512	128	0	128	128

Serial Driver Line 4 Buffer Pool				
	Total	Free	Used	MaxUsed
Buffer Headers	256	128	128	128
Cluster Pool Size: 512	128	0	128	128

These charts show the current usage of the private buffer pools. Private buffer pools are used in various parts of the system to ensure deterministic memory management thus eliminating any contention for memory from the generic heap space.

Copyright © Lantronix, Inc. 2005. All rights reserved.

## Diagnostics: Processes Page

Clicking **Processes** from one of the diagnostics page displays a read-only screen that lists all processes running on the EDS.

- ◆ The **CPU %** column displays the percentage of total CPU cycles a process used in the last two seconds.
- ◆ The **Stacks** column displays the total stack space available to the process and the maximum amount of the stack space the process used since it was started.

Figure 10-10. Diagnostics: Processes Page

**LANTRONIX** EDS4100  
Powered by Evolution OS

Status

Network  
Line  
Tunnel  
DNS  
SNMP  
FTP  
TFTP  
Syslog  
HTTP  
CLI  
Email  
SSH  
SSL  
XML  
Filesystem  
Protocol Stack  
IP Address Filter  
Query Port  
Diagnostics  
System

Hardware MIB-II IP Sockets  
Ping Traceroute DNS Lookup  
Memory Buffer Pools **Processes**

### Diagnostics: Processes

PID	CPU %	Stacks	Process Name
2	0.00%	136/2048	Idle Thread
3	0.00%	228/2048	DNS Cache
4	0.00%	728/4096	EthDB event thread
5	0.00%	212/16192	EthDB maintainer
6	13.51%	884/3072	NetTask-eth0
7	20.68%	232/3072	NetTask-lo0
8	0.00%	472/2048	TFTP Server
9	0.00%	296/2048	FTP Server
10	0.03%	392/2048	Snmp Agent
11	0.00%	3052/14336	Http1
12	0.00%	3052/14336	Http2
13	0.03%	448/14336	Http0
14	0.00%	772/2048	Query Port (7FE)
15	0.32%	220/16384	Network->Serial Daemon Port 1
16	0.01%	300/16384	Serial->Network Daemon Port 1
17	0.00%	488/10208	Accept Mode Daemon Port 1
18	0.00%	312/10208	Connect Mode Daemon Port 1
19	0.32%	220/16384	Network->Serial Daemon Port 2
20	0.01%	300/16384	Serial->Network Daemon Port 2
21	0.00%	488/10208	Accept Mode Daemon Port 2
22	0.00%	312/10208	Connect Mode Daemon Port 2
23	0.32%	220/16384	Network->Serial Daemon Port 3
24	0.01%	300/16384	Serial->Network Daemon Port 3
25	0.00%	488/10208	Accept Mode Daemon Port 3
26	0.00%	312/10208	Connect Mode Daemon Port 3
27	0.32%	220/16384	Network->Serial Daemon Port 4
28	0.01%	300/16384	Serial->Network Daemon Port 4
29	0.00%	488/10208	Accept Mode Daemon Port 4
30	0.00%	312/10208	Connect Mode Daemon Port 4
31	0.00%	688/3104	SMTP Client
32	0.00%	312/2048	Telnet Server
33	0.00%	312/2048	SSH Server
34	0.00%	180/14336	Serial Command Interpreter Port 1
35	0.00%	180/14336	Serial Command Interpreter Port 2
36	0.00%	180/14336	Serial Command Interpreter Port 3
37	0.00%	180/14336	Serial Command Interpreter Port 4

This chart lists all the processes currently running on the system. The CPU % column displays the percentage of total CPU cycles the process used in the last 2 seconds. The Stacks column displays the total stack space available to the process and the maximum amount of the stack space the process used since it was started.

Below the process chart is a CPU Load Graph rendered using the Scalable Vector Graphics (SVG) modularized XML language. The graph is updated every 2 seconds and shows the CPU Load over the last 5 minutes. You can view the raw SVG XML [here](#).

SVG plugin required to view graph.

Copyright © Lantronix, Inc. 2005. All rights reserved.

Below the process chart is a CPU Load Graph that shows the CPU load over the last five minutes. The EDS generates the graph using the Scalable Vector Graphics (SVG) modularized XML language and updates every two seconds. The information area contains a link for viewing the raw SVG XML.

**Note:** The SVG plug-in is available on the Internet.

## System Page

Clicking the **System** link in the menu bar displays the System page. Here you can:

- ◆ Reboot the EDS.
- ◆ Restore factory defaults.
- ◆ Upload new firmware.
- ◆ Assign short and long names to the EDS.
- ◆ Change time settings.

Figure 10-11. System Page

**LANTRONIX**<sup>®</sup>
**EDS32PR**  
Powered by **Evolution OS**

- Status
- Network
- Line
- Tunnel
- DNS
- SNMP
- FTP
- TFTP
- Syslog
- HTTP
- CLI
- Email
- SSH
- SSL
- XML
- Filesystem
- Protocol Stack
- IP Address Filter
- Query Port
- Diagnostics
- System

## System

---

### Reboot Device

---

### Restore Factory Defaults

---

### Upload New Firmware

---

### Name

Short Name:

Long Name:

---

### Change Time Settings

Time Zone:

Date: Year:  Month:  Day:

Time (24hour): Hour:  Min:  Sec:

---

### Current Configuration

<b>Firmware Version:</b>	1.0.0.1R2
<b>Short Name:</b>	EDS32PR
<b>Long Name:</b>	Lantronix EDS32PR
<b>Current Date:</b>	Sat 26 Aug 2006
<b>Current Time:</b>	0:05:40 GMT

When the device is rebooted, your browser should be refreshed and redirected to the main status page after 30 seconds. Note that the redirect will not work as expected if the IP Address of the device changes after reboot.

After setting the configuration back to the factory defaults, the device will automatically be rebooted.

Be careful not to power off or reset the device while uploading new firmware. Once the upload has completed and the new firmware has been verified and flashed, the device will automatically be rebooted.

Copyright © Lantronix, Inc. 2005. All rights reserved.

## System Page

System Page Settings	Description
Reboot Device	Click the <b>Reboot</b> button to reboot the EDS. When the EDS reboots, refresh your Web browser and redirect it to the IP address for the EDS.
Restore Factory Defaults	Click the <b>Factory Defaults</b> button to return the EDS to its factory-default configuration. Appendix C identifies the factory-default configuration. If you restore the factory default configuration, the EDS reboots automatically.
Upload New Firmware	Lets you update the EDS firmware. Do not power off or reset the EDS while uploading new firmware. Once the upload has completed and the new firmware has been verified and flashed, the EDS reboots automatically.
Name	Enter the short name and long name for the EDS. Default short name is EDS and default long name is Lantronix EDS.
Change Time Settings	Lets you specify the system time zone, date, and time. After changing any of these settings, click the <b>Submit</b> button next to the field to accept the change.

## Query Port Page

Clicking the **Query Port** link in the menu bar displays the Query Port page. This page displays statistics and current usage information about the query port server. The query port server is an application that only responds to auto-discovery messages on port 0x77FE. It is used when DeviceInstaller is used to discover the EDS automatically.

Figure 10-12. Query Port Page

**LANTRONIX®** **EDS32PR**  
Powered by **Evolution OS**

Status

**Network**

Line

Tunnel

DNS

SNMP

FTP

TFTP

Syslog

HTTP

CLI

Email

SSH

SSL

XML

Filesystem

Protocol Stack

IP Address Filter

**Query Port**

Diagnostics

System

## Query Port

Query Port Server:  On  Off

---

### Current Configuration and Statistics

Query Port Status:	On (running)
In Valid Queries:	53
In Unknown Queries:	52
In Erroneous Packets:	0
Out Query Replies:	53
Out Errors:	0
Last Connection:	172.18.13.200:28673

This page displays various statistics and current usage information for the Query Port Server. The Query Port Server is a simple application that only responds to auto-discovery messages on port **0x77FE**.

Copyright © Lantronix, Inc. 2005. All rights reserved.

### Query Port Page

Query Port Page Settings	Description
Query Port Server	Select whether the query port server is enabled or disabled. Choices are:  <b>On</b> = query port server is enabled. ( <i>default</i> ) <b>Off</b> = query port server is disabled.

# 11: Advanced Settings

## Email Pages

Clicking the **Email** link in the menu bar displays the Email Statistics page. This page has links at the top for displaying the email configuration and for sending an email. You can configure the email subsystem for delivering email notifications and send an email.

### Email Statistics Page

The Email Statistics page displays when you click **Email** in the menu bar. It also displays when you click **Statistics** at the top of one of the Configuration page. This read-only page shows various statistics and current usage information about the email subsystem.

**To select an email to view its statistics:**

**EDS4100:** Click the desired email at the top of the page.

**EDS8/16/32PR:** Select the email from the **Select Email** drop-down list at the top of the page.

When you transmit an email, the entire conversation with the SMTP server is logged and displayed in the bottom portion of the page. To clear the log, click the **Clear** link.

Figure 11-1. Email Statistics Page

The screenshot shows the LANTRONIX EDS32PR web interface. The top header includes the LANTRONIX logo and 'EDS32PR Powered by Evolution OS'. A sidebar menu on the left lists various system components, with 'Email' highlighted. The main content area features a 'Select Email:' dropdown menu, followed by three tabs: 'Statistics', 'Configuration', and 'Send Email'. The 'Statistics' tab is active, displaying 'Email 1- Statistics' with a table of metrics:

Sent successfully (w/retries):	0 / 0
Not sent due to excessive errors:	0
In transmission queue:	0

Below the table is a 'Log [Clear]' section with the text 'No log data available.' To the right of the main content, a grey box contains explanatory text: 'This page displays various statistics and current usage information of the Email subsystem. When transmitting an Email message the entire conversation with the SMTP server is logged and displayed here. This is a scrolling log in that only the last 100 lines are cached and viewable.' The footer of the page reads 'Copyright © Lantronix, Inc. 2005. All rights reserved.'


## Email Configuration Page

If you click **Configuration** at the top of one of the Email pages, the Email Configuration page displays. Here you can change email configuration settings.

From the **Select Email** drop-down list at the top of the page, select the email whose configuration you want to view. The number of emails is the number of email configurations available. For example, if the highest email number available is 4, then four different email addresses can be used.



Figure 11-2. Email Configuration Page



**EDS32PR**  
 Powered by Evolution OS

---

Status

Network

Line

Tunnel

DNS

SNMP

FTP

TFTP

Syslog

HTTP

CLI

Email

SSH

SSL

XML

Filesystem

Protocol Stack

IP Address Filter

Query Port

Diagnostics

System

Select Email:

---

### Email 1- Configuration

To:

Cc:

From:

Reply-To:

Subject:

File:

Overriding Domain:

Server Port:

Local Port:  or Random

Priority:  Urgent  High  Normal  Low  VeryLow

---

#### Current Configuration

To:	<None>
Cc:	<None>
From:	<None>
Reply-To:	<None>
Subject:	<None>
File:	<None>
Overriding Domain:	<None>
Server Port:	25
Local Port:	Random
Priority:	Normal

When configuring the Email subsystem for delivery of Email notifications, at the very least the **To** and **From** fields must be configured.

The **File** field is used to specify a file on the filesystem that must be sent with all notification Email messages. This file is inserted as the message text, not as an attachment.

The **Overriding Domain** is used to forge the sender Domain Name in the outgoing Email message. This might be necessary, for example, if this device is located behind a firewall whose IP Address resolves to a different Domain Name than this device. For SPAM protection, many SMTP servers perform reverse lookups on the sender IP Address to ensure the Email message is really from who it says it's from.

For testing purposes you can send a Email immediately by pressing the **Send Email** button.

Copyright © Lantronix, Inc. 2005. All rights reserved.

### Email Configuration Page

Email Configuration Page Settings	Description
To (Required)	Enter the email address of the recipient of this message. Separate multiple email addresses with semi-colons.
Cc	Enter the email address to copy this type of email. Separate multiple email addresses with semi-colons.
From (Required)	Enter the email address of the sender of this type of email.
Reply –To	Enter the email address to which replies should be sent.
Subject	Enter the subject of the email.
File	Enter the file on the filesystem that must be sent with all notification email messages. The file is inserted as the message text, not as an attachment.
Overriding Domain	Enter the sender's domain name that will be forged in the outgoing email message. This domain name may be needed if this device is located behind a firewall whose IP address resolves to a different domain name than this device. For SPAM protection, many SMTP servers perform reverse lookups on the sender IP address to ensure the email message is really from whom it says it is from.
Server Port	Enter the SMTP server port number. The default is a random port number. Usually, the port number is 25, but it is configurable.
Local Port or Random	Enter the local port to use for email alerts. The default is a random port number.
Priority	Select the priority level for the email alert.

To test your configuration, you can send an email immediately by clicking **Send Email** at the top of the page.

## CLI Pages

Clicking the **CLI** link in the menu bar displays the Command Line Interface Statistics page. This page has two links at the top for viewing statistics and for viewing and changing configuration settings.

### Command Line Interface Statistics Page

The Command Line Interface Statistics page displays when you click **CLI** in the menu bar. It also displays when you click **Statistics** at the top of the CLI Configuration page. This read-only page shows the current connection status of the CLI servers listening on the Telnet and SSH ports. When a connection is active:

- ◆ The remote client information displays.
- ◆ The number of bytes that have been sent and received displays.
- ◆ A **Kill** link can be used to terminate the connection.

Figure 11-3. Command Line Interface Statistics Page

The screenshot shows the Lantronix EDS32PR web interface. The left sidebar contains a navigation menu with the following items: Status, Network, Line, Tunnel, DNS, SNMP, FTP, TFTP, Syslog, HTTP, CLI (highlighted), Email, SSH, SSL, XML, Filesystem, Protocol Stack, IP Address Filter, Query Port, Diagnostics, and System. The main content area is titled 'Command Line Interface Statistics' and has two tabs: 'Statistics' (selected) and 'Configuration'. Below the tabs are two tables:

Telnet Status	
Server Status:	Enabled (Waiting)
Local Port:	23
Last Connection:	<None>
Uptime:	2 days 21:29:33.019
Total Bytes In:	0
Total Bytes Out:	0
Current Connections:	<None>

SSH Status	
Server Status:	Enabled (Waiting)
Local Port:	22
Last Connection:	<None>
Uptime:	2 days 21:29:33.017
Total Bytes In:	0
Total Bytes Out:	0
Current Connections:	<None>

On the right side of the page, there is a text box explaining that the page displays the current connection status of the CLI servers listening on the Telnet and SSH ports. It also notes that when a connection is active, remote client information is displayed, including the number of bytes sent and received. A 'Clear' link is mentioned as being present to kill the connection. At the bottom of the page, there is a copyright notice: 'Copyright © Lantronix, Inc. 2005. All rights reserved.'

## Command Line Interface Configuration Page

If you click **Configuration** at the top of the Command Line Interface Statistics page, the Command Line Interface Configuration page displays. Here you can change CLI configuration settings.

Under **Current Configuration**, **Password** has a **Delete** link. If you click **Delete**, a message asks whether you are sure you want to delete this information. Click **OK** to proceed or **Cancel** to cancel the operation.

Figure 11-4. Command Line Interface Configuration Page

The screenshot shows the Lantronix EDS32PR web interface. The left sidebar contains a navigation menu with items like Status, Network, Line, Tunnel, DNS, SNMP, FTP, TFTP, Syslog, HTTP, CLI, Email, SSH, SSL, XML, Filesystem, Protocol Stack, IP Address Filter, Query Port, Diagnostics, and System. The main content area is titled 'Command Line Interface Configuration' and includes a 'Submit' button. To the right, there is explanatory text about Telnet and SSH settings.

**Command Line Interface Configuration**

Telnet Access:  On  Off

Telnet Port:

SSH Access:  On  Off

SSH Port:

Password:

Enable Password:

Quit connect line:

**Current Configuration**

Telnet Access:	Enabled
Telnet Port:	23
SSH Access:	Enabled
SSH Port:	22
Password:	<None>
Enable Level Password:	<None>
Quit connect line:	<control>L

Both the **Telnet Port** and **SSH Port** used by the CLI servers can be overridden.  
 The **Password** is used for initial Telnet login access.  
 For the SSH server, the **SSH Server Authorized Users** are used for initial login access.  
 The **Enable Password** is used for access to the 'enable' level within the CLI.  
 The **Quit connect line** string is used to terminate a connect line session and resume the CLI. Type <control> before any key to be pressed while holding down the Ctrl key, for example, <control>L.

Copyright © Lantronix, Inc. 2005. All rights reserved.

## Command Line Interface Configuration Page

Command Line Interface Configuration Page Settings	Description
Telnet Access	Select whether Telnet access is enabled. Choices are: <b>On</b> = Telnet access is enabled. ( <i>default</i> ) <b>Off</b> = Telnet access is disabled.
Telnet Port	Enter the number of the port on which the EDS listens for incoming Telnet connections. Default is 23.
SSH Access	Select whether Secure Shell (SSH) access is enabled. Choices are: <b>On</b> = SSH access is enabled. ( <i>default</i> ) <b>Off</b> = SSH access is disabled.
SSH Port	Enter the number of the port on which the EDS listens for incoming SSH connections. Default is 22.
Password	Enter the password that must be specified for the initial Telnet login session. Default is PASS.

Command Line Interface Configuration Page Settings	Description
Enable Password	Enter the password that must be specified to access the “enable” level in the CLI. Default is disabled.
Quit connect line	Enter a string to terminate a connect line session and resume the CLI. Type <b>&lt;control&gt;</b> before any key the user must press when holding down the <b>Ctrl</b> key. An example of a such a string is <b>&lt;control&gt;L</b> .

## XML Pages

The EDS can be configured using an XML configuration record. Clicking the **XML** link in the menu bar displays the XML page. This page has three links at the top for exporting an XML configuration record, exporting an XML status record, and importing an XML configuration record.

### XML Configuration Record: Export System Configuration Page

The XML Configuration Record: Export System Configuration page displays when you click **XML** in the menu bar. It also displays when you click **Export XML Configuration Record** at the top of one of the other XML pages. Here you can export the current system configuration in XML format. The generated XML file can be imported later to restore a configuration. It can also be modified and imported to update the configuration on this EDS unit or another. The XML data can be exported to the browser window or to a file on the filesystem.

Figure 11-5. XML Configuration Record: Export System Configuration Page

LANTRONIX<sup>®</sup>

EDS4100

Powered by Evolution OS

- Status
- Network
- Line
- Tunnel
- DNS
- SNMP
- FTP
- TFTP
- Syslog
- HTTP
- CLI
- Email
- SSH
- SSL
- XML
- Filesystem
- Protocol Stack
- IP Address Filter
- Query Port
- Diagnostics
- System

Export XML  
Configuration  
Record

Export XML  
Status Record

Import XML  
Configuration  
Record

## XML Configuration Record: Export System Configuration

Export XCR data to browser  
 Export XCR data to the filesystem:  
 Filename

**GROUPS TO EXPORT:**

<input type="checkbox"/> arp:eth0	<input type="checkbox"/> cli
<input type="checkbox"/> clock	<input type="checkbox"/> command mode passwords
<input type="checkbox"/> device	<input type="checkbox"/> email:1
<input type="checkbox"/> email:2	<input type="checkbox"/> email:3
<input type="checkbox"/> email:4	<input type="checkbox"/> ethernet:eth0
<input type="checkbox"/> firmware	<input type="checkbox"/> ftp server
<input type="checkbox"/> http authentication:/	<input type="checkbox"/> http server
<input type="checkbox"/> icmp	<input type="checkbox"/> interface:eth0
<input type="checkbox"/> ip filter:eth0	<input type="checkbox"/> line:1
<input type="checkbox"/> line:2	<input type="checkbox"/> line:3
<input type="checkbox"/> line:4	<input type="checkbox"/> query port
<input type="checkbox"/> reboot	<input type="checkbox"/> reload factory defaults
<input type="checkbox"/> rss	<input type="checkbox"/> serial command mode:1
<input type="checkbox"/> serial command mode:2	<input type="checkbox"/> serial command mode:3
<input type="checkbox"/> serial command mode:4	<input type="checkbox"/> snmp
<input type="checkbox"/> ssh client	<input type="checkbox"/> ssh command mode
<input type="checkbox"/> ssh server	<input type="checkbox"/> ssl
<input type="checkbox"/> syslog	<input type="checkbox"/> tcp
<input type="checkbox"/> telnet command mode	<input type="checkbox"/> tftp server
<input type="checkbox"/> tunnel accept:1	<input type="checkbox"/> tunnel accept:2
<input type="checkbox"/> tunnel accept:3	<input type="checkbox"/> tunnel accept:4
<input type="checkbox"/> tunnel aes accept:1	<input type="checkbox"/> tunnel aes accept:2
<input type="checkbox"/> tunnel aes accept:3	<input type="checkbox"/> tunnel aes accept:4
<input type="checkbox"/> tunnel aes connect:1	<input type="checkbox"/> tunnel aes connect:2
<input type="checkbox"/> tunnel aes connect:3	<input type="checkbox"/> tunnel aes connect:4
<input type="checkbox"/> tunnel connect:1	<input type="checkbox"/> tunnel connect:2
<input type="checkbox"/> tunnel connect:3	<input type="checkbox"/> tunnel connect:4
<input type="checkbox"/> tunnel disconnect:1	<input type="checkbox"/> tunnel disconnect:2
<input type="checkbox"/> tunnel disconnect:3	<input type="checkbox"/> tunnel disconnect:4
<input type="checkbox"/> tunnel modem:1	<input type="checkbox"/> tunnel modem:2
<input type="checkbox"/> tunnel modem:3	<input type="checkbox"/> tunnel modem:4
<input type="checkbox"/> tunnel packing:1	<input type="checkbox"/> tunnel packing:2
<input type="checkbox"/> tunnel packing:3	<input type="checkbox"/> tunnel packing:4
<input type="checkbox"/> tunnel serial:1	<input type="checkbox"/> tunnel serial:2
<input type="checkbox"/> tunnel serial:3	<input type="checkbox"/> tunnel serial:4
<input type="checkbox"/> tunnel start:1	<input type="checkbox"/> tunnel start:2
<input type="checkbox"/> tunnel start:3	<input type="checkbox"/> tunnel start:4
<input type="checkbox"/> tunnel stop:1	<input type="checkbox"/> tunnel stop:2
<input type="checkbox"/> tunnel stop:3	<input type="checkbox"/> tunnel stop:4

This page is used for exporting the current system configuration in XML format. The generated XML file can be imported at a later time to restore the configuration. Also, the XML file can be modified and imported to update the configuration on this device or another.

The XML data can be exported to the browser window or to a file on the filesystem. If no configuration **groups** are specified then all groups will be exported.

Copyright © Lantronix, Inc. 2005. All rights reserved.

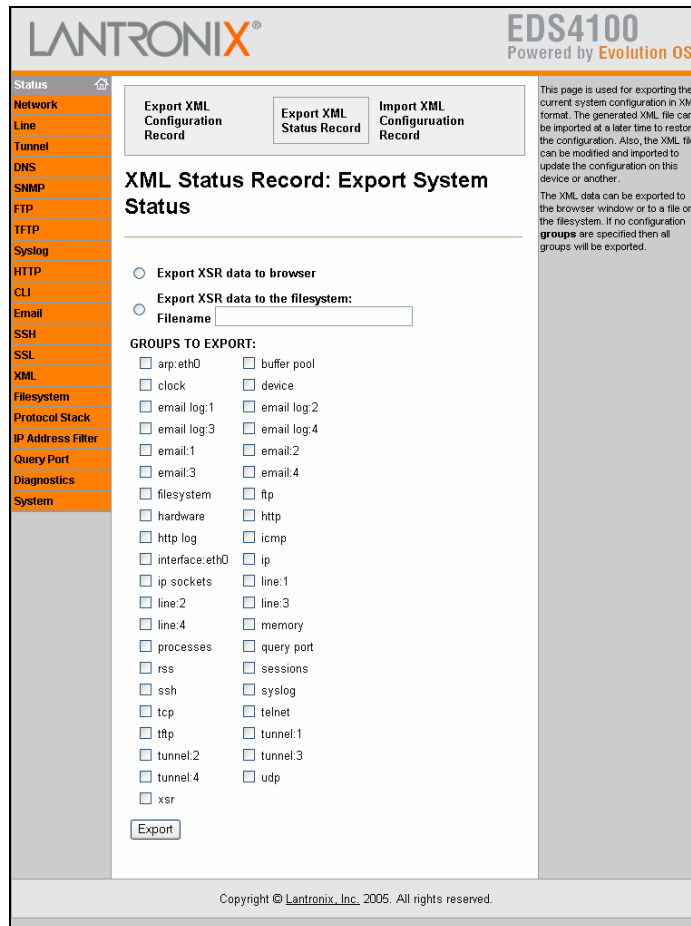
Configuration Record: Export System Configuration Page

XML Configuration Record: Export System Configuration Page Settings	Description
Export XCR data to browser	Select this option to export the XCR data to a Web browser.
Export XCR data to the filesystem	Select this option to export the XCR data to a filesystem. If you select this option, enter a file name for the XML configuration record.
Groups to Export	Check the configuration groups that are to be exported to the XML configuration record. If no groups are checked, all groups will be exported.

XML Status Record: Export System Status

If you click **XML Status Record** at the top of an XML page, the XML Status Record: Export System Status page displays. Here you can export the current system status in XML format. The XML data can be exported to the browser window or to a file on the filesystem.

Figure 11-6. XML Status Record: Export System Status Page



## XML Status Record: Export System Status Page

XML Status Record: Export System Status Page Settings	Description
Export XSR data to browser	Select this option to export the XML status record to a Web browser.
Export XSR data to the filesystem	Select this option to export the XML status record to a filesystem. If you select this option, enter a file name for the XML status record.
Groups to Export	Check the configuration groups that are to be exported into the XML status record. If no groups are checked, all groups will be exported.

**XML: Import System Configuration Page**

If you click **Import XML Configuration Record** at the top of an XML page, the XML: Import System Configuration page displays. Here you can import a system configuration from an XML file.

The XML data can be imported from a file on the filesystem or uploaded using HTTP. The groups to import can be specified by toggling the respective group item or entering a filter string. When toggling a group item, all instances of that group will be imported. The filter string can be used to import specific instances of a group. The text format of this string is:

```
<g>:<i>;<g>:<i>;...
```

Each group name <g> is followed by a colon and the instance value <i>. Each <g>:<i> value is separated with a semicolon. If a group has no instance, specify the group name <g> only.



Figure 11-7. XML: Import System Configuration Page

LANTRONIX®

EDS4100

Powered by Evolution OS

---

Status 🏠

Network

Line

Tunnel

DNS

SNMP

FTP

TFTP

Syslog

HTTP

CLI

Email

SSH

SSL

XML

Filesystem

Protocol Stack

IP Address Filter

Query Port

Diagnostics

System

Export XML Configuration Record
Export XML Status Record
Import XML Configuration Record

## XML: Import System Configuration

---

**Import entire external XCR file:**

---

**Import XCR file from the filesystem:**

Filename

**Groups and Instances to Import:**

Filter

**WHOLE GROUPS TO IMPORT:**

<input type="checkbox"/> arp	<input type="checkbox"/> cli
<input type="checkbox"/> clock	<input type="checkbox"/> command mode passwords
<input type="checkbox"/> device	<input type="checkbox"/> email
<input type="checkbox"/> ethernet	<input type="checkbox"/> execute
<input type="checkbox"/> exit cli	<input type="checkbox"/> ftp server
<input type="checkbox"/> http authentication uri	<input type="checkbox"/> http server
<input type="checkbox"/> icmp	<input type="checkbox"/> interface
<input type="checkbox"/> ip filter	<input type="checkbox"/> line
<input type="checkbox"/> query port	<input type="checkbox"/> reboot
<input type="checkbox"/> restore factory configuration	<input type="checkbox"/> rss
<input type="checkbox"/> serial command mode	<input type="checkbox"/> snmp
<input type="checkbox"/> ssh client	<input type="checkbox"/> ssh command mode
<input type="checkbox"/> ssh server	<input type="checkbox"/> ssl
<input type="checkbox"/> syslog	<input type="checkbox"/> tcp
<input type="checkbox"/> telnet command mode	<input type="checkbox"/> test
<input type="checkbox"/> tftp server	<input type="checkbox"/> tunnel accept
<input type="checkbox"/> tunnel aes accept	<input type="checkbox"/> tunnel aes connect
<input type="checkbox"/> tunnel connect	<input type="checkbox"/> tunnel disconnect
<input type="checkbox"/> tunnel modem	<input type="checkbox"/> tunnel packing
<input type="checkbox"/> tunnel serial	<input type="checkbox"/> tunnel start
<input type="checkbox"/> tunnel stop	

This page is used for importing system configuration from an XML file.

The XML data can be imported from a file on the filesystem or uploaded using HTTP. If no configuration **groups** are specified then all groups will be imported.

The **groups** to import can be specified by toggling the respective group item or typing in a **Filter** string. When toggling a group item, all instances of that group will be imported. The **Filter** string can be used to import specific instances of a group. The textual format of this string is:

```
<g>:<i>;<g>:<i>;...
```

Each group name <g> is followed by a colon and the instance value <i> and each <g>:<i> value is separated by a semi-colon. If a group has no instance then only the group name <g> should be specified.

---

Copyright © Lantronix, Inc. 2005. All rights reserved.

## XML: Import System Configuration Page

XML: Import System Configuration Page Settings	Description
Import entire external XCR file	Enter the path and file name of the entire external XCR file you want to import or use the <b>Browse</b> button to select the XCR file.
Import XCR file from filesystem	Enter the filename of the XCR file that has certain groups you want to import.
Groups and Instances to Import	If required, enter the filter string for importing specific instances of a group.
Whole Groups to Import	Check the configuration groups that are to be imported into the XML configuration record. If no groups are checked, all groups will be imported.

## Protocol Stack Page

Clicking the **Protocol Stack** link in the menu bar displays the Protocol Stack page. Here you can configure lower level network stack-specific configuration settings.

Under **Current State**, there is a **Clear** link to remove all addresses and a **Remove** link to remove the individual address shown. If you click **Clear** or **Remove**, a message asks whether you are sure you want to perform the operation. Click **OK** to proceed or **Cancel** to cancel the operation.

Figure 11-8. Protocol Stack Page

LANTRONIX®

EDS32PR

Powered by Evolution OS

- Status
- Network
- Line
- Tunnel
- DNS
- SNMP
- FTP
- TFTP
- Syslog
- HTTP
- CLI
- Email
- SSH
- SSL
- XML
- Filesystem
- Protocol Stack
- IP Address Filter
- Query Port
- Diagnostics
- RTC
- System

### TCP

Send RSTs:  On  Off

#### Current State

Send RSTs:	On
Total Out RSTs:	3
Total In RSTs:	2

### ICMP

Enable:  On  Off

#### Current State

Enable:  On

### ARP

ARP Timeout:  seconds

#### Current State

ARP Timeout:

### ARP Cache

IP Address:

MAC Address:

#### Current State [Clear]

Address	Age	MAC Address	Type	Interface
172.18.0.1 <a href="#">[Remove]</a>	22.622	00:d0:04:02:c0:00	Dynamic	1
172.18.25.105 <a href="#">[Remove]</a>	37.106	00:20:4a:08:a1:74	Dynamic	1
172.18.100.40 <a href="#">[Remove]</a>	0.5	00:01:02:4f:d6:d5	Dynamic	1

This page contains lower level Network Stack specific configuration items.

**TCP**  
The **Send RSTs** boolean is used to turn on/off sending of TCP RST messages.

**ICMP**  
The **Enable** boolean is used to turn on/off processing of ICMP messages. This includes both incoming and outgoing messages.

**ARP**  
The **ARP Timeout** specifies how long a MAC Address will remain in the cache before being removed.

**ARP Cache**  
The ARP Cache can be manipulated manually by adding new entries and deleting existing ones.

Copyright © Lantronix, Inc. 2005. All rights reserved.

## Protocol Stack Page

Protocol Stack Page Settings	Description
<b>TCP</b>	
Send RSTs	<p>RST is a TCP control bit that informs the receiving TCP stack to end a connection immediately. However, sending this bit may pose a security risk. Select whether you want the RST control bit sent to end a connection immediately. Choices are:</p> <p><b>On</b> = the RST bit is sent. (<i>default</i>)</p> <p><b>Off</b> = the RST bit is not sent.</p> <p>After selecting an option, click <b>Submit</b>.</p>
<b>ICMP</b>	
	<p>Internet Control Message Protocol (ICMP) can be used as an error-reporting protocol between two hosts. This setting specifies whether incoming and outgoing ICMP messages are processed. Choices are:</p> <p><b>On</b> = ICMP messages are processed. (<i>default</i>)</p> <p><b>Off</b> = ICMP messages are not processed.</p> <p>After selecting an option, click <b>Submit</b>.</p>
<b>ARP</b>	
	<p>Enter the maximum number of seconds that a MAC address will remain in cache before being removed. Default is 00:01:00. (one minute). After selecting an option, click <b>Submit</b>.</p>
<b>ARP Cache</b>	
IP Address	Enter the IP address of the entry to be added to the Address Resolution Protocol (ARP) cache.
MAC Address	Enter the MAC address of the entry to be added to the ARP cache. After entering an IP address and a MAC address, click <b>Submit</b> .

## IP Address Filter Page

Clicking the **IP Address Filter** link in the menu bar displays the IP Address Filter page. Here you can specify the IP addresses and subnets allowed to send data to the EDS. All packets sent from IP addresses not on this list are ignored and discarded. By default, the IP address list is empty, so all addresses are allowed.

The network mask and IP address settings you specify on this page determine the range of IP addresses that can access the EDS. For example:

- ◆ An IP address of 10.0.0.0 and a network mask of 255.0.0.0 allows any device with an IP address in the 10.x.x.x range to access the EDS.
- ◆ An IP address of 192.168.1.1 with a network mask of 255.0.0.0 causes the EDS to allow all IP addresses in the range of 192.x.x.x.
- ◆ An IP address of 192.168.1.1 with a network mask of 255.255.255.0 only allows IP addresses in the range of 192.168.1.x to access the EDS.

Figure 11-9. IP Address Filter Page



IP Address Filter Page

IP Address Filter Page Settings	Description
IP Address	Enter the IP address that is allowed to send packets to the EDS. If using DHCP with BOOTP, enter the IP address of the DHCP/BOOTP server.
Network Mask	Enter the network mask associated with the IP address that is allowed to send packets to the EDS.

## 12: Updating Firmware

Lantronix periodically releases updates to the firmware to fix problems or provide feature upgrades.

### Obtaining Firmware

Obtain the most up-to-date firmware and release notes for the EDS from the Lantronix Web site (<http://www.lantronix.com/support/downloads.html>) or by using anonymous FTP (<ftp://ftp.lantronix.com/>).

### Upgrading Using DeviceInstaller

#### Loading New Firmware

1. Download the EDS firmware from <http://www.lantronix.com/support/downloads.html>.
2. Unzip the files and save them to a directory on your PC

#### Updating the Boot Loader from DeviceInstaller

**Note:** If the unzipped files contain a file named **edsxxboot.rom.gz** (where xx is the model designation 4100, 16, or 32), then the boot loader must be updated before the standard firmware.

1. Start DeviceInstaller. (See [Starting DeviceInstaller](#) on page 30.)
2. Open the EDS folder in the left Window pane.
3. Select the EDS that you would like to upgrade.
4. Click the **Web Configuration** tab and click **Go**.
5. Enter the **User name** and **Password**. The default user name is **admin** with a default password of **PASS** (all caps).
6. On the menu bar, click **System**. The System page displays.
3. Under **Upload New Firmware**, click **Browse** and navigate to the directory where you saved the EDS firmware.

**Note:** If the **edsxxboot.rom.gz** file does not exist in the downloaded firmware directory, proceed directly to step 8 in the **Updating firmware** section below.

8. Select **edsxxboot.rom.gz** and click **Upload**.

## Updating Firmware

1. Open DeviceInstaller. (See [Starting DeviceInstaller](#) on page 30.)
2. Open the EDS folder in the left Window pane.
3. Select the EDS that you would like to upgrade.
4. Click the **Web Configuration** tab and click **Go**.
5. Enter the **User name** and **Password**. The default user name is **admin** with a default password of **PASS** (all caps).
6. On the menu bar, click **System**. The System page displays.
4. Under **Upload New Firmware**, click **Browse** and navigate to the directory where you saved the EDS firmware.
5. Select **edsxx.rom.gz** and click **Upload**.

## A: Factory Default Configuration

This appendix lists the EDS factory-default configuration. The types of settings are in alphabetical order.

### Network Configuration Settings

Network Configuration Parameters	Network Configuration Settings
BOOTP Client	Off (disabled)
DHCP Client	On (enabled)
IP Address	0.0.0.0 (auto-IP if DHCP fails)
Network Mask	0.0.0.0 (auto if DHCP fails)
Gateway	0.0.0.0
MAC Address	Specified by manufacturer
Hostname	None
Domain	None
DHCP Client ID	None
Ethernet	Auto speed, auto duplex

### Serial Port Line Settings

Serial Port Line Parameters	Serial Port Line Settings
Status	Enabled
Baud Rate	9600 baud
Parity	None
Data Bits	8
Stop Bits	1



Serial Port Line Parameters	Serial Port Line Settings
Flow Control	None
Xon char	0x11 (\17)
Xoff char	0x13 (\19)
Command Mode	Disabled
Use Serial String	Off (disabled)
Echo Serial String	On (enabled)
Wait Time (milliseconds)	5000 milliseconds
Serial String (text or binary)	None
Signon Message	None

## Tunnel Settings

### Serial Settings

Serial Parameters	Serial Settings
Buffer Size	2048 bytes
Read Timeout (milliseconds)	200 milliseconds
Wait for Read Timeout	Disabled

### Start/Stop Characters

Start/Stop Character Parameters	Start/Stop Character Settings
Start Character	None
Stop Character	None
Echo Start Character	Off
Echo Stop Character	Off

## Accept Mode

Accept Mode Parameters	Accept Mode Settings
Accept Mode	Enabled
Local Port	Port 1 = 10001, Port 2 = 10002, Port 3 = 10002, and so forth.
Protocol	TCP
Flush Serial Data	Disabled
Block Serial Data	Off
Block Network Data	Off
TCP Keep Alives	45 seconds
Email on Connect	None
Email on Disconnect	None
Password	None
Prompt for Password	Off

## Connect Mode

Connect Mode Parameters	Connect Mode Settings
Connect Mode	Disabled
Remote Address	None
Remote Port	None
Local Port	Random
Protocol	TCP
Reconnect Timer	15000 milliseconds
Flush Serial Data	Disabled
SSH Username	None
Block Serial Data	Off
Block Network Data	Off
TCP Keep Alives	45 seconds

Connect Mode Parameters	Connect Mode Settings
Email on Connect	None
Email on Disconnect	None

### Disconnect Mode

Disconnect Mode Parameters	Disconnect Mode Settings
Mode	Disabled
Timeout	60000 milliseconds
Flush Serial Data	Disabled

### Packing Mode

Packing Mode Parameters	Packing Mode Settings
Mode	Disabled
Timeout	1000 milliseconds
Threshold	512 bytes
Send Character	None
Trailing Character	None

### Modem Emulation

Modem Emulation Parameters	Modem Emulation Settings
Echo Pluses	Off
Echo Command	On
Verbose Response Codes	On
Response Codes	Text
Error Unknown Commands	Off
Optional Connect String	None

## AES Keys

AES Key Parameters	AES Key Settings
Accept Mode AES Keys: Encrypt Key	None
Accept Mode AES Keys: Decrypt Key	None
Connect Mode AES Keys: Encrypt Key	None
Connect Mode AES Keys: Decrypt Key	None

## DNS Settings

DNS Parameters	DNS Settings
Primary Server	None
Secondary Server	None

## SNMP Settings

SNMP Parameters	SNMP Settings
SNMP Agent	Running
Read Community	Public
Write Community	Private
System Contact	None
System Name	EDSxxxx (xxxx = 4100, 8PR, 16PR, 32PR)
System Description	Lantronix EDSxxxx (xxxx = 4100, 8PR, 16PR, 32PR)
System Location	None
Enable Traps	On
Primary TrapDest IP	None
Secondary TrapDest IP	None

## FTP Settings

FTP Parameters	FTP Settings
FTP Server	On
Username	admin
Password	PASS

## TFTP Settings

TFTP Parameters	TFTP Settings
TFTP Server	On
Allow TFTP File Creation	Disabled

## Syslog Settings

Syslog Parameters	Syslog Settings
Syslog Status	Off
Host	None
Local Port	514
Remote Port	514
Severity to Log	None

## HTTP Settings

### Configuration

HTTP Configuration Parameters	HTTP Settings
HTTP Server	On
HTTP Port	80
HTTPS Port	443
Max Timeout	10 seconds
Max Bytes	40960
Logging	On
Max Log Entries	50
Log Format	%h %t "%r" %s %B "%{Referer}i" "%{User-Agent}i"

### Authentication

HTTP Authentication Parameters	HTTP Authentication Settings
URI	/
Realm	config
AuthType	Digest
Username	admin
Password	PASS

### RSS

HTTP RSS Parameters	HTTP RSS Settings
RSS Feed	Off
Persistent	Off
Max Entries	100

## CLI Settings

### Telnet

CLI Telnet Parameters	CLI Telnet Settings
Telnet Access	Enabled
Telnet Port	23
SSH Access	Enabled
SSH Port	22
Password	None
Enable Password	None
Quit Connect Line	<control>L

## Email Settings

Email Parameters	Email Settings
To	None
Cc	None
From	None
Reply –To	None
Subject	None
File	None
Overriding Domain	None
Server Port	25
Local Port or Random	Random
Priority	Normal

## Query Port Settings

Query Port Parameters	Query Port Settings
Query Port Server	On

## Diagnostics Settings

### Ping

Diagnostics Ping Parameters	Diagnostic Ping Settings
Count	3
Timeout	5 seconds

## System Settings

System Parameters	System Settings
Short Name	EDSxxxx (xxxx = 4100, 16PR, or 32PR)
Long Name	Lantronix EDSxxxx (xxxx 4100, 16PR, or 32PR)
Time Zone	GMT +0.00 (GMT)
Date	None
Time (24 hour)	None

## IP Address Filter

IP Address Parameters	IP Address Settings
IP Address	None
Network Mask	None



## B: Technical Specifications

### EDS4100

EDS4100 Technical Specifications

Category	EDS4100 Specifications
<b>CPU</b>	Intel® XScale IXP420 Network Processor running at 266MHz 32k Instruction Cache 32k Data Cache
<b>Flash</b>	8 MBytes Flash
<b>RAM</b>	32 MBytes SDRAM
<b>EEPROM</b>	2 KB
<b>Firmware</b>	Upgradable via the Web Manager, TFTP, or FTP
<b>Serial Interface</b>	4 DB9M serial ports: 2 RS232, 2 RS232/422/485, software selectable Software-selectable standard baud rates from 300 to 230k baud. Customizable baud rate support for non-standard serial speeds.
<b>Serial Line Formats</b>	Data bits: 7 or 8 Stop bits: 1 or 2 Parity: odd, even, none
<b>Modem Control</b>	CTS, RTS, DTR, DCD
<b>Flow Control</b>	Xon/Xoff (software), CTS/RTS (hardware), None
<b>Power Input</b>	9-30 VDC - Barrel connector 42-56 VDC - Screw Terminal PoE compliant power source - 802.3af (when populated)
<b>Network Interface</b>	RJ45 Ethernet 10Base-T or 100Base-TX (auto-sensing and hard coded, auto-crossover), full- or half duplex
<b>Compliance</b>	Ethernet: Version 2.0/IEEE 802.3 (electrical) Ethernet II frame type IEEE 802.3af (when PoE is populated)

Category	EDS4100 Specifications (cont'd)
<b>Dimensions</b>	Height: 12.7 cm (5.0 in) Width: Without mounting brackets 17.65 cm (6.95 in) Width: With mounting brackets 20.14 cm (7.93 in) Depth: 3.81 cm (1.5 in)
<b>Weight</b>	.86 Kg (1.9 lb)
<b>Temperature</b>	0 to +55C operating temperature -40 to +70C storage temperature
<b>Relative Humidity</b>	10 to 90%, non-condensing
<b>Case</b>	Metal enclosure with removable wall mounts
<b>Protocols Supported</b>	ARP, UDP/IP, TCP/IP, Telnet, ICMP, SNMP, DHCP, BOOTP, TFTP, Auto IP, SMTP, FTP, DNS, Traceroute, and HTTP
<b>Management</b>	Internal web server, SNMP v2C (MIB-II, RS232MIB), Serial login, Telnet login, XML
<b>Security</b>	SSL v3, SSH v2 MD5, SHA-1 Rijndael/AES 128-bit encryption 3DES encryption ARC4 128-bit encryption Password protection IP address filtering Hardened OS and stack
<b>Internal Web Server</b>	Serves static and dynamic CGI-based pages and Java applets Storage capacity: 6 MB using industry standard file system
<b>System Software</b>	Windows-based DeviceInstaller configuration software and Windows-based Com Port Redirector
<b>LEDs</b>	10Base-T and 100Base-TX Link Ethernet Activity Serial Transmit Data Serial Receive Data Power Status
<b>EMC Standards</b>	FCC CFR 47 Part 15 Subpart B, ICES-003 Issue 4, AS/NZS CISPR 22, VCCI V-3, EN55022, EN61000-3-2, EN61000-3-3, EN55024, EN61000-4-2, EN61000-4-3, EN61000-4-4, EN61000-4-5, EN61000-4-6, EN61000-4-8, EN61000-4-11
<b>Safety Standards</b>	UL 60950-1, CSA-22.2 No. 60950-1-03, EN60950-1, CB Report - IEC 60950-1
<b>Product Label Markings</b>	FCC Part 15 Statement Class A Device, ICES-003 Class A Device, C-Tick, VCCI, CE Marking, UL-CUL Mark, TUV-GS Mark

## EDS8/16/32PR

## EDS8/16/32PR Technical Specifications

Category	EDS8/16/32PR Specifications
<b>CPU</b>	Intel® XScale IXP420 Network Processor running at 266MHz 32k Instruction Cache 32k Data Cache
<b>Flash</b>	8 MBytes Flash
<b>RAM</b>	32 MBytes SDRAM
<b>EEPROM</b>	2 KB
<b>Firmware</b>	Upgradable via the Web Manager, TFTP, or FTP
<b>Serial Interface</b>	Software-selectable RJ45 serial ports Software-selectable standard baud rates from 300 to 230k baud. Customizable baud rate support for non-standard serial speeds.
<b>Serial Line Formats</b>	Data bits: 7 or 8 Stop bits: 1 or 2 Parity: odd, even, none
<b>Modem Control</b>	CTS, RTS, DTR, DSR
<b>Flow Control</b>	Xon/Xoff (software), CTS/RTS (hardware), None
<b>Power Input</b>	100-240 VAC, 50-60 Hz IEC-type cord 20 Watts
<b>Network Interface</b>	RJ45 Ethernet 10Base-T or 100Base-TX (auto-sensing and hard coded, auto-crossover), full- and half-duplex
<b>Compliance</b>	Ethernet: Version 2.0/IEEE 802.3 (electrical) Ethernet II frame type
<b>Dimensions (LxWxH)</b>	30.5 x 43.8 x 43.4 cm (12 x 17.25 x 1.75 in.), 1U
<b>Weight</b>	10 lb maximum
<b>Temperature</b>	0° to +55°C operating temperature -40° to +66°C storage temperature
<b>Relative Humidity</b>	5 to 95%, non-condensing

Category	EDS8/16/32PR Specifications (cont'd)
<b>Case</b>	Metal enclosure with removable rack mounts
<b>Protocols Supported</b>	ARP, UDP/IP, TCP/IP, Telnet, ICMP, SNMP, DHCP, BOOTP, TFTP, Auto IP, SMTP, FTP, DNS, Traceroute, and HTTP
<b>Management</b>	Internal web server, SNMP v2C (MIB-II, RS232MIB), Serial login, Telnet login, XML
<b>Security</b>	SSL v3, SSH v2 MD5, SHA-1 Rijndael/AES 128-bit encryption 3DES encryption ARC4 128-bit encryption Password protection IP address filtering Hardened OS and stack
<b>Internal Web Server</b>	Serves static and dynamic CGI-based pages and Java applets Storage capacity: 6 MB using industry standard file system
<b>System Software</b>	Windows-based DeviceInstaller configuration software and Windows-based Secure Com Port Redirector
<b>LEDs</b>	10Base-T and 100Base-TX Link Ethernet Activity Serial Transmit Data Serial Receive Data Power Diagnostics
<b>EMC Standards</b>	FCC CFR 47 Part 15 Subpart B, ICES-003 Issue 4, AS/NZS CISPR 22, VCCI V-3, EN55022, EN61000-3-2, EN61000-3-3, EN55024, EN61000-4-2, EN61000-4-3, EN61000-4-4, EN61000-4-5, EN61000-4-6, EN61000-4-8, EN61000-4-11
<b>Safety Standards</b>	UL 60950-1, CSA-22.2 No. 60950-1-03, EN60950-1, CB Report - IEC 60950-1
<b>Product Label Markings</b>	FCC Part 15 Statement Class A Device, ICES-003 Class A Device, C-Tick, VCCI, CE Marking, UL-CUL Mark, TUV-GS Mark

## C: Networking and Security

This chapter describes the following networking and security concepts as they relate to the EDS:

- ◆ SSL — described below.
- ◆ SSH — see page [143](#)
- ◆ Serial tunneling — see page [144](#)

This chapter concludes with a description of modem emulation (page [147](#)).

### SSL

Secure Sockets Layer (SSL) is an open-standard security protocol that provides privacy through encryption, server authentication, and message integrity. From its introduction in 1994, SSL has become the industry standard for securing e-commerce transactions over TCP/IP connections. And it is easy to see why.

Imagine mailing a letter in a clear envelope that anyone could see. If the envelope contained a check, credit card, or other valuable information, some nefarious individual could steal the letter or change its contents. Information traveling over networks, including the Internet, is just as vulnerable.

Prior to SSL, packets of information would travel networks in full view of anyone who could access the data. As the World Wide Web grew and gained in popularity, a solution became necessary for securing e-commerce transactions over the Internet. The solution would have to enable Internet consumers to reliably identify the Internet vendors (e-commerce servers) with whom they transact business while, at the same time, protect the confidentiality of the consumers' sensitive information as it traversed the Internet. With the advent of SSL, personal information that could be seen by anyone with access to view it could now be secure.

#### Benefits of SSL

The following list summarizes the benefits of SSL:

- ◆ Widely implemented standard for e-commerce applications
- ◆ Reduces the complexities associated with keeping user information confidential
- ◆ Works with existing Web servers and browsers
- ◆ Eliminates the need for additional software applications
- ◆ Provides high level of security
- ◆ Platform and O/S neutral
- ◆ Allows server authentication via certificates

## How SSL Works

SSL uses cryptography to deliver authentication and privacy to message transmission over the Internet. SSL permits the communication of client/server applications without eavesdropping and message tampering.

SSL runs on layers between application protocols (HTTP, SMTP, etc.) and the TCP transport protocol. To set up an SSL connection, a TCP/IP connection must be established first. The SSL connection sets up a secure channel within the TCP/IP connection in which all traffic between the client and server is encrypted. All the calls from the application layer to the TCP layer are replaced with calls to the SSL layer, with the SSL layer handling communication with the TCP layer.

SSL is most commonly used with HTTP (thus forming HTTPS). Web sites protected by SSL start with a URL that begins with “https” and displays a padlock icon at the bottom of the page (and for Mozilla Firefox in the address bar as well).

When a Web browser accesses a domain secured by SSL, an SSL handshake authenticates the server and client, and establishes an encryption method and a unique session key. Once this handshake has been completed, the client and server can begin a secure session that guarantees message privacy and message integrity.

SSL uses Digital-Certificate technology to identify target servers reliably and uses encryption to protect the confidentiality of information passing between client and server. You can configure the EDS to use an SSL certificate for the HTTP server. The certificate can be created elsewhere and uploaded to the EDS, or it can be automatically generated as a self-signed certificate on the EDS. For more information about uploading a new certificate or create a new self-signed certificate, see [SSL](#) on page 92.

**Note:** When uploading the certificate and the private key, be sure the private key is not compromised in transit.

The following steps summarize how SSL works:

1. A client contacts a server secured by SSL.
2. In response to the client request, the server sends its certificate to the client.
3. The client generates a master key, which it encrypts with the server's public key and transmits the encrypted master key back to the server.
4. The server recovers the master key and authenticates itself to the client by returning a message authenticated with the master key. Subsequent data is encrypted and authenticated with keys derived from this master key.

## Digital Certificates

Authentication with SSL is achieved with a Digital Certificate issued and signed by a Certificate Authority (CA) and stored on the server. Without a certificate signed by a CA, the server cannot be reliably identified to the client, yet a connection can still proceed if allowed.

The Digital Certificate resides on a secure server and is used to encrypt data and identify the Web site. The Digital Certificate verifies that a site belongs to who it claims to belong to and contains information about the certificate holder, the domain that the certificate was issued to, the name of the Certificate Authority who issued the certificate, the root and the country it was issued in. In addition to proving the veracity of a site, the Digital

Certificate provides the receiver with a way to encode a reply. Digital Certificates come in 40-bit and 128-bit versions.

There are two principal ways that a Digital Certificate can be obtained. It can be bought from a certificate vendor or a user can "self-sign" his or her own certificate. With the latter method, a user can use various tools, both open source and proprietary, to sign his or her own Digital Certificate, saving the time and expense of going through a certificate vendor.

## SSH

Like SSL, Secure Shell (SSH) is a protocol that provides secure encrypted communications over unsecured TCP/IP networks such as the Internet. SSH allows for secure access to remote systems, eliminating potential security breaches such as spoofing and eavesdropping or hijacking of sessions. However, SSH differs significantly from SSL and, in fact, cannot communicate with SSL. The two are different protocols, though they have some overlap in how they accomplish similar goals.

### How Does SSH Authenticate?

SSH authenticates using one or more of the following:

- ◆ Password (the `/etc/passwd` or `/etc/shadow` in UNIX)
- ◆ User public key (RSA or DSA, depending on the release)
- ◆ Hostbased (`.rhosts` or `/etc/hosts.equiv` in SSH1 or public key in SSH2)

### What Does SSH Protect Against?

SSH provides strong authentication and secure communications over insecure channels. It also provides secure connections that protect a network from attacks such as:

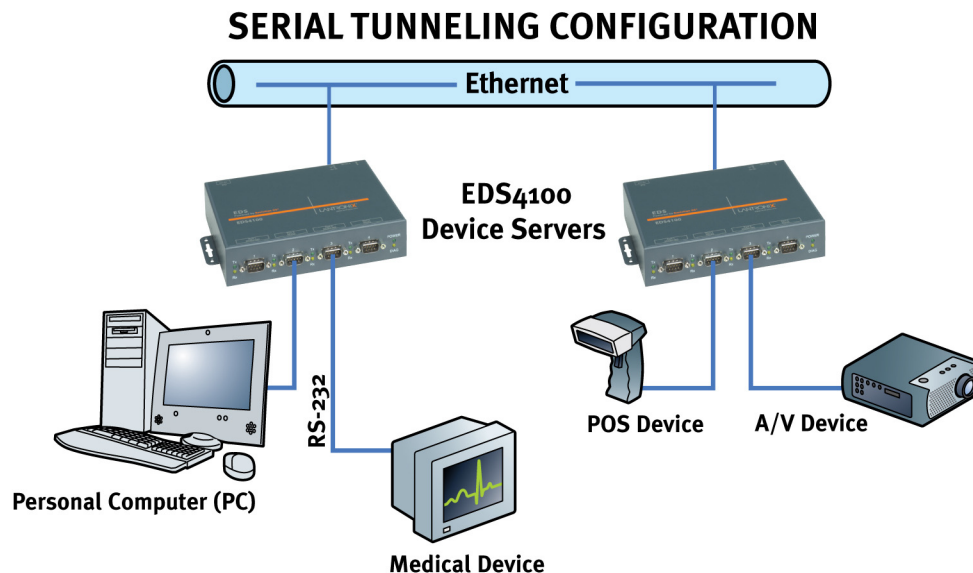
- ◆ IP spoofing, where a remote host sends packets that pretend to originate from another, trusted host. SSH even protects against a spoofer on the local network that is pretending to be a router to the outside.
- ◆ IP source routing, where a host pretends that an IP packet comes from another, trusted host.
- ◆ DNS spoofing, where an attacker forges name server records.
- ◆ Interception of cleartext passwords and other data by intermediate hosts.
- ◆ Manipulation of data by people in control of intermediate hosts.
- ◆ Attacks based on listening to authentication data and spoofed connections to the server.

## Tunneling

Tunneling provides a way to create a connection between two serial devices across an untrusted network so the devices can share data. The sharing of information is achieved through a direct connection (or “serial tunnel”) between the two devices that encapsulates, authenticates, and encrypts the serial data into TCP packets and sends them across the Ethernet network. In this way, two previously isolated and non-networked devices can securely and effectively communicate and exchange information and operate with existing installed software applications or devices that are configured to run independent of an Ethernet network. And because the tunnel can be secure, anyone who tries to monitor the conversation between the two devices would see encrypted, unintelligible data.

The figure below shows how a pair of device servers can be used in tandem to provide transparent serial tunneling across an Ethernet network. In this example, a POS device in a store collects data and sends it to a device server attached to a POS serial port. The device server forwards the collected data, through an encrypted tunnel established over the Ethernet network, to a device server connected to a remote PC. The data received at the remote device server is decrypted and forwarded to the PC’s serial port and received at the remote PC. In this way, serial data that goes in one end comes out at the other end.

Example of an Encrypted Tunnel





## Tunneling and the EDS

Each EDS serial port supports two concurrent tunneling connections, Connect mode and Accept mode. These connections operate independently of the other EDS serial ports.

- ◆ In Connect mode, the EDS actively makes a connection. The receiving node on the network must listen for the Connect mode's connection. By default, Connect mode is disabled.
- ◆ In Accept mode, the EDS listens for a connection. A node on the network initiates the connection. By default, Accept mode is enabled.
- ◆ Disconnect mode defines how an active connection is disconnected. The parameters used to drop the connection are user configurable. The EDS's Disconnect mode disconnects both Accept mode and Connect mode connections on a serial port when it observes the defined event occur on that port.

When any character arrives through the serial port, it gets copied to both the Connect mode connection and Accept mode connection if both are active.

## Connect Mode

For Connect mode to work:

- ◆ Connect mode must be enabled on the EDS (see [Tunnel – Connect Mode Page](#) on page 59).
- ◆ A remote station (node) must be configured for Connect mode.
- ◆ A remote TCP or UDP port must be configured.

When Connect mode is enabled, it remains on until it is ended by Disconnect mode.

Connect mode supports the following protocols:

- ◆ TCP
- ◆ AES encryption over UDP
- ◆ AES encryption over TCP
- ◆ SSH (the EDS is the SSH client)
- ◆ UDP (available only in Connect mode since it is a connectionless protocol)

For AES encryption, both the encrypt key and the decrypt key must be specified. The encrypt key is used with data sent from the EDS, while the decrypt key is used when the EDS receives data. Both keys can have the same value.

If the remote address or port is not configured and Connect mode is set to UDP, the EDS accepts packets from any device on the network and sends packets to the last device that sent it packets. To ensure the EDS does not accept UDP packets from all devices on the network, you must configure the remote address and port. When the remote port and station are configured, the EDS ignores data from other sources.

To configure SSH, the SSH client username must be configured. In Connect Mode, the EDS is the SSH client. Ensure the EDS's SSH client username is configured on the SSH server before using it with the EDS.

Connect Mode has six variations:

- ◆ Disabled (no connection)
- ◆ Enabled (always makes a connection)
- ◆ Active if it sees any character from the serial port (makes a connection upon receiving any character)
- ◆ Active if it sees a specific (configurable) character from the serial port
- ◆ Modem emulation (controlled by modem commands)
- ◆ Modem control asserted (makes a connection when the modem central signal on the serial line becomes active)

For the “any character” or “specific character” connection states, the EDS waits and retries the connection if the connection cannot be made. Once it makes a connection and then disconnects, it does not reconnect until it sees any character or the start character again (depending on the configured setting).

## Accept Mode

In Accept mode, the EDS waits for a connection. The configurable local port is the port the remote device connects to for this connection. There is no remote port or address. The default local port is 10001 for serial port 1, 10002 for serial port 2, 10003 for serial port 3, and so forth.

Accept Mode supports the following protocols:

- ◆ SSH (EDS is the server in Accept Mode). For this protocol, the SSH server host keys and at least one SSH authorized user must be configured.
- ◆ TCP
- ◆ AES encryption over TCP

Accept Mode has the following options:

- ◆ Disabled (close the connection)
- ◆ Enabled (always listening for a connection)
- ◆ Active if it receives any character from the serial port
- ◆ Active if it receives a specific (configurable) character from the serial port (same start character as Connect Mode’s start character)
- ◆ Modem control signal (when the modem control on the serial line corresponding to the tunnel becomes active)

## Disconnect Mode

Disconnect mode ends Accept mode and Connect mode connections. When disconnecting, the EDS shuts down connections gracefully.

The following three settings end a connection:

- ◆ The EDS receives the stop character.
- ◆ The timeout period elapses and no activity is going in or out of the EDS. Both Accept mode and Connect mode must be idle for the time frame.
- ◆ The EDS observes the modem control inactive setting.

To clear out data from the serial buffers upon disconnecting, configure the EDS to flush serial data (see [Tunnel – Disconnect Mode Page](#) on page 62).

## Packing Mode

Packing mode takes data from the serial port, groups it together, and sends it out to nodes on the network. The groupings may be configured by size or by time intervals.

The following settings are configurable for Packing mode:

- ◆ Enable or disable Packing mode
- ◆ Packing mode timeout. Data that is packed for a specified period of time before being sent out.
- ◆ Packing mode threshold. When the buffer fills to a specified amount of data and the timeout has not elapsed, the EDS packs the data and sends it out.
- ◆ Send character. Similar to a start or stop character, the EDS packs data until it sees the send character. When it sees the send character, the EDS sends the packed data and the send character in the packet.
- ◆ Trailing character. If a trailing character is defined, this character is appended to data put on the network immediately following the send character.

## Modem Emulation

The EDS supports Modem Emulation mode for devices that transmit modem AT commands. The EDS supports two different modes:

- ◆ **Command Mode:** The EDS serial ports accept modem commands that instruct the EDS to perform an action such as start or drop a connection.
- ◆ **Data Mode:** Serial data received in the EDS serial port is sent through the active network connection.

The Tunnel – Modem Emulation page lets you configure modem emulation settings for up to four tunnels for the EDS4100, 16 for the EDS16PR, and 32 for the EDS32PR (see [Tunnel – Modem Emulation Page](#) on page 65). Each tunnel can have different settings.

**Note:** When the EDS serial port is in Modem Emulation mode, the serial port remains in Command mode until an active tunnel starts. Once an active tunnel starts, the serial port remains in Data mode until the connection is dropped or the serial port is placed in Command mode by issuing the modem command +++.

## Command Mode

The Modem Emulation's Command mode supports the standard AT command set. For a list of available commands from the serial or telnet login, enter AT?. Use ATDT, ATD, and ATDP to establish a connection:

+++	Switches to command mode if entered from serial port during connection.
AT?	Help.
ATDT<Address Info>	Establishes the TCP connection to socket (<IP>/<port>).
ATDP<Address Info>	See ATDT.
ATD	Like ATDT. Dials default connect mode remote address and port.
ATO	Switches to data mode if connection still exists. Vice versa to '+++'.
ATE <i>n</i>	Switches echo in command mode (off - 0, on - 1).
ATH	Disconnects the network session.
ATI	Displays modem information.
ATS0 = <i>n</i>	Accept incoming connection. ( <i>n</i> = 0: disable, <i>n</i> = 1: connect automatically, <i>n</i> = 2+: connect with ATA command (basically wait for the user or application to issue a command to "pick up the phone"))
ATQ <i>n</i>	Quiet mode (0 - enable results code, 1 - disable result codes)
ATV <i>n</i>	Verbose mode (0 - numeric result codes, 1 - text result codes)
ATZ	Restores the current state from the setup settings.
A/	Repeat last valid command.

These commands allow the EDS to emulate a modem. The EDS ignores valid AT commands that do not apply to the EDS and sends an OK response code.

In Command mode, the EDS can make a connection to the remote host and using the remote address and remote port information specified on the Tunnel – Connect Mode page (see [Tunnel – Connect Mode Page](#) on page 59).

When making a connection from the EDS using an ATDT or ATDP command, full or partial IP addresses can be used. If a partial IP address is used, the EDS uses the remote address and port as configured in the Connect Mode settings.

For the following examples, we assume that the remote address is 192.168.16.10 and the port is set to 10001 in the Connect mode settings:

- ◆ Entering **ATDT** alone causes the EDS to connect to the IP address and remote port configured in Connect Mode.
- ◆ Entering **ATDT 119.25.50** causes the EDS to assume the first octet in the IP address and connects to the remote IP address 192.119.25.50, port 10001.

(Since the remote port was not specified in the **ATDT** command, the remote port defined under Connect mode is used.)

- ◆ Entering **ATDT 28.150** causes the EDS to assume the first two octets in the IP address and connects to the remote IP address 192.168.28.150, port 10001.
- ◆ Entering **ATDT 150** causes the EDS to assume the first three octets and connects to the remote IP address 192.168.16.150, port 10001.
- ◆ Entering **ATDT 28.150:10012** causes the EDS to assume the first two octets in the IP address and connects to the remote IP address 192.168.28.150, port 10012.

**Note:** *If you add 10012 after the IP address segment, port 10012 is used instead of the port defined in Connect mode.*

By default, the +++ characters are not passed through the connection. To pass them through the connection, enable Echo Pluses on the Tunnel - Modem Emulation page (see [Tunnel – Modem Emulation Page](#) on page 65).

## ***D: Technical Support***

If you are unable to resolve an issue using the information in this documentation:

### **Technical Support US**

Check our online knowledge base or send a question to Technical Support at

<http://www.lantronix.com/support>.

### **Technical Support Europe, Middle East, Africa**

Phone: +33 1 39 30 41 72

Email: [mailto:eu\\_techsupp@lantronix.com](mailto:eu_techsupp@lantronix.com) or [mailto:eu\\_support@lantronix.com](mailto:eu_support@lantronix.com)

Firmware downloads, FAQs, and the most up-to-date documentation are available at

<http://www.lantronix.com/support>

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

- ◆ Your name, and your company name, address, and phone number
- ◆ Lantronix model number
- ◆ Lantronix serial number
- ◆ Software version (on the first screen shown when you Telnet to port 23)
- ◆ 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)

## E: Lantronix Cables and Adapters

Lantronix P/N	Description	Applications
500-103	6' RJ45-to DB9F	<p>Included with EDS8/16/32PR for setup or device connectivity.</p> <p>Connects the RJ45 RS232 serial ports of EDS8/16/32PR to a DB9M DTE interface of a PC or serial device.</p>
200.2062	Cable Ethernet CAT5; RJ45, 2 m (6.6 ft)	<p>Connects the EDS8/16/32PR Ethernet ports to an Ethernet switch/hub or is used for cascading from one EDS8/16/32PR to another.</p> <p>Connects the EDS8/16/32PR serial RJ45 RS232 ports to a device using one of the adapters listed below.</p>
200.2063	Cable Ethernet CAT5; RJ45, 5 m (16.4 ft)	<p>Connects the EDS8/16/32PR Ethernet ports to an Ethernet switch/hub or is used for cascading from one EDS8/16/32PR to another.</p> <p>Connects the EDS8/16/32PR serial RJ45 RS232 ports to a device using one of the below listed adapters.</p>
200.2064	Cable Ethernet CAT5; RJ45, 10 m (32.8 ft)	<p>Connects the EDS8/16/32PR Ethernet ports to an Ethernet switch/hub or is used for cascading from one EDS8/16/32PR to another.</p> <p>Connects the EDS8/16/32PR serial RJ45 RS232 ports to a device using one of the adapters listed below.</p>
200.2065	Cable Ethernet CAT5; RJ45, 15 m (49.2 ft)	<p>Connects the EDS8/16/32PR Ethernet ports to an Ethernet switch/hub or is used for cascading from one EDS8/16/32PR to another.</p> <p>Connects the EDS8/16/32PR serial RJ45 RS232 ports to a device using one of the adapters listed below.</p>
200.2066A	Adapter RJ45-to-DB25M	Allows a standard straight-pinned CAT5 cable to connect the EDS8/16/32PR RJ45 serial ports to the DB25F DCE interface of a serial device.
200.2067A	Adapter RJ45-to-DB25F	Allows a standard straight-pinned CAT5 cable to connect the EDS8/16/32PR RJ45 serial ports to the DB25M DTE interface of a serial device.
200.2069A	Adapter RJ45-to-DB9M	Allows a standard straight-pinned CAT5 cable to connect the EDS8/16/32PR RJ45 serial ports to the DB9F DCE interface of a serial device.
200.2070A	Adapter RJ45-to-DB9F	Allows a standard straight-pinned CAT5 cable to connect the EDS8/16/32PR to the DB9M DTE interface of a PC or serial device.

## **F: Compliance**

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

**Manufacturer's Name & Address:**

Lantronix 15353 Barranca Parkway, Irvine, CA 92618 USA

**Declares that the following product:**

**Product Name Model:** EDS4100 4 Port Device Server, EDS16PR 16 Port Device Server, and EDS32PR 32 Port Device Server

**Conforms to the following standards or other normative documents:**

**Radiated and conducted emissions**

Class B limits of EN 55022:1998  
EN55024: 1998 + A1: 2001

**Direct & Indirect ESD**

EN61000-4-2: 1995

**RF Electromagnetic Field Immunity**

EN61000-4-3: 1996

**Electrical Fast Transient/Burst Immunity**

EN61000-4-4: 1995

**Surge Immunity**

EN61000-4-5: 1995

**RF Common Mode Conducted Susceptibility**

EN61000-4-6: 1996

**Power Frequency Magnetic Field Immunity**

EN61000-4-8: 1993

**Voltage Dips and Interrupts**

EN61000-4-11: 1994

**Manufacturer's Contact:**

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



## Lithium Battery Notice

CAUTION: DANGER OF EXPLOSION IF BATTERY IS INCORRECTLY REPLACED. REPLACE ONLY WITH THE SAME OR EQUIVALENT TYPE RECOMMENDED BY THE MANUFACTURER. DISCARD USED BATTERIES ACCORDING TO THE MANUFACTURER'S INSTRUCTIONS.

ACHTUNG: WIRD BEIM BATTERIEWECHSEL EINE FALSCH E BATTERIE EINGESETZT, BESTEHT EXPLOSIONSGEFAHR. SETZEN SIE NUR EINE BATTERIE DES GLEICHEN ODER EINES ENTSPRECHENDEN, VOM HERSTELLER EMPFOHLENE TYP S EIN. ENTSORGEN SIE VERBRAUCHETE BATTERIEN GEMÄSS DEN ANWEISUNGEN DES HERSTELLERS.

## Installationsanweisungen

### Rackmontage

Bei Montage in ein geschlossenes Rack oder in ein Rack mit mehreren Einheiten ist unter Umständen eine weitere Prüfung erforderlich. Folgende Punkte sind zu berücksichtigen.

1. Die Umgebungstemperatur innerhalb des Racks kann höher sein als die Raumtemperatur. Die Installation muss so durchgeführt werden, dass der für den sicheren Betrieb erforderliche Luftstrom nicht beeinträchtigt wird. In dieser Umgebung darf die maximale Temperatur von 50°C nicht überschritten werden. Dabei sind auch die maximalen Auslegungstemperaturen zu berücksichtigen.
2. Die Installation ist so durchzuführen, dass auch bei ungleichmäßiger Lastverteilung die Stabilität gewährleistet bleibt.

### Energiezufuhr

Anhand der Angaben auf dem jeweiligen Typenschild ist sicherzustellen, dass keine Überlastung an der Einspeisung erfolgt, die den Überstromschutz und die Versorgungsleitungen beeinträchtigt.

### Erdung

Eine zuverlässige Schutzerdung dieser Ausrüstung muss gewährleistet sein. Dies gilt besonders bei Anschluss an Mehrfachsteckdosen.

## Installation Instructions

### Rack Mounting

If rack mounted units are installed in a closed or multi-unit rack assembly, they may require further evaluation by certification agencies. You must consider the following items:

1. The ambient within the rack may be greater than the room ambient. Installation should be such that the amount of air flow required for safe operation is not

compromised. The maximum temperature for the equipment in this environment is 50°C. Consideration should be given to the maximum rated ambient.

2. Installation should be such that a hazardous stability condition is not achieved due to uneven loading.

### **Input Supply**

Check nameplate ratings to assure there is no overloading of supply circuits that have an effect on overcurrent protection and supply wiring.

### **Grounding**

Reliable earthing of this equipment must be maintained. Particular attention should be given to supply connections when connecting to power strips, rather than direct connections to the branch circuit strips.

## G: Warranty

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

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

\* \* \* \*

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

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

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

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

For details on the Lantronix warranty replacement policy, go to our web site at [www.lantronix.com/support/warranty](http://www.lantronix.com/support/warranty).

## Index

- Accept mode, 146
  - Settings, 56
- Accessing Web Manager, 34
- AES key settings, 67
- Applications, 17
- Authentication settings, 79
- Authorized users,SSH server, 88
- Browsing the filesystem, 96
- Buffer pool diagnostics, 105
- Certificate, self-signed, 92
- CLI pages, 114
  - Configuration, 115
  - Statistics, 114
- Client users
  - SSH server, 89
- Command mode, 51, 148
- Compliance, 152
- Components of Web Manager pages, 42
- Configuration
  - CLI, 115
  - HTTP, 77
  - Line, 49
  - Methods, 32
  - Network, 44
  - Telnet, 32
  - Web Manager, 32
  - XML, 33
- Connect mode, 59, 145
- Copying files to the filesystem, 96
- Device Status page, 43
- DeviceInstaller, 30
- Diagnostics pages, 98
  - Buffer pool, 105
  - DNS lookup, 103
  - Hardware, 98
  - IP sockets, 100
  - Memory, 104
  - MIB-II network statistics, 99
  - Ping, 101
  - Processes, 106
  - Traceroute, 102
- Digital Certificates, 142
- Directories, creating, 96
- Disconnect mode, 62, 146
- DNS
  - Lookup, 103
  - Page, 70
- EDS
  - Applications, 17
  - Diagnostics, 98
  - Factory default configuration, 128
  - Properties, 30
  - Rebooting, 107
  - Restoring factory defaults, 107
  - Short and long names, 107
  - Updating firmware, 107
- EDS16/32PR
  - Features, 14
  - Hardware components, 26
  - Installation, 28
  - Overview, 13
  - Package contents, 25
  - Reset button, 28
  - Serial ports, 27
  - Technical specifications, 139
  - User-supplied Items, 25
- EDS4100
  - Ethernet port, 22
  - Features, 13
  - Hardware components, 20
  - Installation, 23
  - LEDs, 22
  - Overview, 12
  - Package contents, 19
  - Reset button, 23
  - Serial ports, 21
  - Terminal block connector, 22
  - User-supplied Items, 19
- Email pages, 111
- Ethernet port, 27
- Evolution OS™, 14
- Exporting
  - System configuration record, 117
  - System status, 119

- Factory default configuration, 128
- Features, 13
- Files
  - Copying, 96
  - Creating, 96
  - Moving, 96
  - Transferring to/from a TFTP server, 96
  - Uploading via HTTP, 96
- Filesystem pages, 95
  - Browser, 96
- Firmware
  - Loading new, 107
  - Obtaining, 126
  - Updating, 107
- FTP page, 72
- Hardware diagnostics, 98
- Host key settings, SSH server, 84
- HTTP pages, 76
  - Authentication, 79
  - Configuration, 77
  - RSS, 82
  - Statistics, 76, 111
  - Uploading a file to the filesystem, 96
- Installation
  - EDS16/32PR, 25, 28
  - EDS4100, 19, 23
- IP Address Filter page, 124
- IP socket diagnostics, 100
- Known hosts, SSH server, 86
- LEDs
  - EDS16/32PR, 27
  - EDS4100, 22
- Line Settings pages, 47
  - Command Mode, 51
  - Configuration, 49
  - Statistics, 48
- Loading new firmware, 107
- Long name, 107
- Memory diagnostics, 104
- MIB-II network statistics, 99
- Modem emulation
  - Command mode, 148
  - Overview, 147
  - Settings, 65
- Moving files to the filesystem, 96
- Names, short and long, 107
- Navigating through the
  - Web Manager, 36
- Network Configuration page, 44
- Obtaining firmware, 126
- Packing mode, 64, 147
- Pinging an IP address, 101
- Processes diagnostics, 106
- Properties, 30
- Protocol Stack page, 122
- Query Port page, 109
- Rebooting, 107
- Reset button
  - EDS4100, 23
- Reset button
  - EDS16/32PR, 28
- Restoring factory defaults, 107
- RSS settings, 82
- Self-signed certificate, 92
- Short name, 107
- SNMP page, 71
- Specifications, 139
- SSH
  - How it authenticates, 143
  - Overview, 143
  - What it protects against, 143
- SSH pages, 84
  - SSH client known hosts, 86
  - SSH client users, 89
  - SSH server authorized users, 88
  - SSH server host keys, 84
- SSL, 92
  - Benefits, 141
  - Digital Certificates, 142
  - How it works, 142
  - Overview, 141
- Start character settings, 55
- Statistics
  - CLI, 114
  - HTTP, 76, 111
  - Line, 48
  - MIB-II network, 99
  - Tunnel, 52
- Stop character settings, 55
- Syslog page, 75
- System configuration record
  - Exporting, 117
  - Importing, 120
- System page, 107
- System status, Exporting, 119
- Technical specifications, 139
- Telnet configuration, 32
- TFTP page, 74
- TFTP server, transferring files, 96
- Traceroute, 102
- Transferring files to/from a TFTP server, 96
- Tunnel pages

- Accept mode, 56
- AES keys, 67
- Connect mode, 59
- Disconnect mode, 62
- Modem emulation, 65
- Packing mode, 64
- Serial settings, 53
- Start and stop characters, 55
- Statistics, 52
- Tunneling
  - Accept mode, 146
  - Connect mode, 145
  - Disconnect mode, 146
  - Overview, 144
  - Packing mode, 147
- Updating firmware, 107
- Uploading a file to the filesystem, 96
- Warranty, 155
- Web Manager
  - Accessing, 34
  - Navigating through, 36
  - Overview, 32
  - Page components, 42
  - Page summary, 36
- Web Manager pages
  - CLI, 114
  - Device Status, 43
  - Diagnostics, 98
  - DNS, 70
  - Email, 111
  - Filesystem, 95
  - FTP, 72
  - HTTP, 76
  - IP Address Filter, 124
  - Line Settings, 47
  - Network Configuration, 44
  - Protocol Stack, 122
  - Query Port, 109
  - SNMP, 71
  - SSH, 84
  - SSL, 92
  - Syslog, 75
  - System, 107
  - TFTP, 74
  - Tunnel, 52
  - XML, 117
- XML
  - Configuration, 33
- XML pages, 117
  - Export system configuration record, 117
  - Export system status, 119
  - Import system configuration record, 120