

LANTRONIX®



MatchPort™
AR A R C H I T E C T

MatchPort AR User Guide

Copyright and Trademark

© 2007, 2008, 2009, 2010 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.

Warranty

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

Contacts

Lantronix Corporate Headquarters

167 Technology Drive
Irvine, CA 92618, USA
Toll Free: 800-526-8766
Phone: 949-453-3990
Fax: 949-450-7249

Technical Support

Online: 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.

Disclaimer and Revisions

The information in this guide may change without notice. The manufacturer assumes no responsibility for any errors that may appear in this guide. For the latest revision of this product document, please check our online documentation at www.lantronix.com/support/documentation.

Compliance

This product has been designed to comply with the limits for a Class B digital device pursuant to Part 15 of FCC and EN55022:1998 Rules when properly enclosed and grounded. These limits are designed to provide reasonable protection against radio interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with this guide, may cause interference to radio communications. For more information, see [Compliance on page 148](#).

Revision History

Date	Rev.	Comments
June 2007	A	Initial document.
September 2008	B	Technical updates throughout, corresponding to firmware release 1.1.0.0.R6.
May 2009	C	Technical updates throughout; added RoHS notice.
May 2010	D	Updated for firmware release 5.1.0.0R10. Added VIP Access and Multiple Hosts in Connect Mode.

Table of Contents

Copyright and Trademark	2
Warranty	2
Contacts	2
Disclaimer and Revisions	2
Compliance	2
Revision History	3
1: About This Guide	12
Chapter and Appendix Summaries	12
Conventions	13
Additional Documentation	13
2: Overview	15
Key Product Features	15
Applications	15
Protocol Support	16
Evolution OS™	16
Software Features	16
Modem Emulation	16
Web-Based Configuration and Troubleshooting	17
Command-Line Interface (CLI)	17
VIP Access	17
SNMP Management	17
XML-Based Architecture and Device Control	17
Really Simple Syndication (RSS)	17
Enterprise-Grade Security	17
Terminal Server/Device Management	18
Troubleshooting Capabilities	18
Configuration Methods	18
Addresses and Port Numbers	19
Hardware Address	19
IP Address	19
Port Numbers	19
Product Information Label	19
3: Using DeviceInstaller	21
Accessing MatchPort AR using DeviceInstaller	21
Device Details Summary	21
4: Configuration Using Web Manager	23
Accessing Web Manager	23
Web Manager	25
Navigating the Web Manager	26

5: Network Settings	28
Network 1 Interface Status _____	28
Network 1 Interface Configuration _____	29
Network 1 Ethernet Link _____	30
6: Line and Tunnel Settings	32
Line Settings _____	32
Line Statistics _____	32
Line Configuration _____	33
Line Command Mode _____	35
Tunnel Settings _____	37
Tunnel Statistics _____	38
Serial Settings _____	39
Packing Mode _____	40
Packing Mode using Timeout _____	42
Packing Mode using Send Character _____	43
Accept Mode _____	44
Connect Mode _____	46
Multiple Hosts _____	51
Host List Promotion _____	53
Disconnect Mode _____	54
Modem Emulation _____	55
Command Mode _____	55
7: Terminal and Host Settings	59
Terminal Settings _____	59
Network Terminal Configuration _____	59
Line Terminal Configuration _____	60
Host Configuration _____	62
8: Configurable Pins Manager	64
Overview _____	64
Default Groups _____	64
Custom Groups _____	64
Configurable Pins _____	64
Change CPs _____	65
CPM Groups _____	67
View CP Group Status _____	67
Add Custom CP Groups _____	67
Remove Custom CP Groups _____	69
Remove CPs from CP Groups _____	69
9: Services Settings	70
DNS Status and Cache _____	70
PPP Configuration _____	71

SNMP Configuration	74
FTP	75
TFTP	77
Syslog	78
HTTP	79
HTTP Statistics	79
HTTP Configuration	80
HTTP Authentication	83
RSS	84
LPD	86
LPD Statistics	86
LPD Configuration	87
10: Security Settings	89
SSH Server Host Keys	89
SSH Server Authorized Users	91
SSH Client Known Hosts	93
SSH Client Users	94
SSL Cipher Suites	96
SSL Certificates	97
SSL RSA or DSA	97
SSL Certificates and Private Keys	98
SSL Utilities	98
SSL Configuration	99
11: VIP	102
Obtain a Bootstrap File	102
Import the Bootstrap File	102
Enable VIP	103
Configure Tunnels to Use VIP	103
VIP Statistics	103
VIP Configuration	104
12: Maintenance and Diagnostics Settings	106
Filesystem	106
Filesystem Statistics and Actions	106
Filesystem Browser	107
Protocol Stack	110
TCP	110
IP	111
ICMP	112
ARP	113
IP Address Filter	114
Query Port	115

Diagnostics	116
Hardware	116
MIB-II	117
IP Sockets	118
Ping	118
Traceroute	120
DNS Lookup	121
Memory	122
Buffer Pools	123
Processes	123
System	125
13: Advanced Settings	127
Email Statistics	127
Email Configuration	128
Command Line Interface	129
CLI Statistics	130
CLI Configuration	130
XML Configuration	132
XML Export Configuration	132
XML Export Status	134
XML Import Configuration	135
Import Configuration from External File	136
Import Configuration from Filesystem	137
Import Line(s) from Single Line Settings on the Filesystem	139
14: Branding the MatchPort AR	142
Web Manager Customization	142
Short and Long Name Customization	142
15: Updating Firmware	144
A: Technical Support	145
B: Binary to Hexadecimal Conversions	146
Converting Binary to Hexadecimal	146
Conversion Table	146
Scientific Calculator	147
C: Compliance	148
Declaration of Conformity	148
RoHS Notice	149

List of Figures

Figure 2-1 MatchPort AR Product Information Label	20
Figure 4-1 MatchPort AR Web Manager Home Page	24
Figure 4-2 Components of a Typical Web Manager Page	25
Figure 5-1 Network1 (eth0) Interface Status Web Page	28
Figure 5-2 Network 1 (eth0) Interface Configuration Web Page	29
Figure 5-4 Network1 (eth0) Ethernet Link Web Page	31
Figure 6-1 Line 1 Statistics Web Page	33
Figure 6-2 Line 1 Configuration Web Page	34
Figure 6-3 Line 1 Command Mode Web Page	36
Figure 6-4 Tunnel 1 Statistics Web Page	38
Figure 6-5 Tunnel 1 Serial Settings Web Page	39
Figure 6-6 Tunnel 1 Packing Mode Web Page	41
Figure 6-7 Tunnel 1 Packing Mode (Timeout)	42
Figure 6-8 Tunnel 1 Packing Mode (Send Character)	43
Figure 6-9 Tunnel 1 Accept Mode Web Page	45
Figure 6-10 Tunnel Connect Mode Page	48
Figure 6-11 Host Mode	51
Figure 6-12 Host 2 Configuration Fields	52
Figure 6-13 Host List Promotion	53
Figure 6-14 Tunnel 1 Disconnect Mode Web Page	54
Figure 6-15 Tunnel 1 Modem Emulation Web Page	57
Figure 7-1 Terminal on Network Configuration Web Page	59
Figure 7-2 Terminal on Line 1 Configuration Web Page	61
Figure 7-3 Host Configuration Web Page	62
Figure 8-1 CPM CPs Page	65
Figure 8-2 CPM Groups Page	68
Figure 9-1 DNS Status and Cache Web Page	71
Figure 9-2 PPP Configuration Web Page	72
Figure 9-3 SNMP Web Page	74
Figure 9-4 FTP Web Page	76
Figure 9-5 TFTP Server Web Page	77
Figure 9-6 Syslog Web Page	78
Figure 9-7 HTTP Statistics Web Page	80
Figure 9-8 HTTP Configuration Web Page	81
Figure 9-9 HTTP Authentication Web Page	83
Figure 9-10 RSS Web Page	85
Figure 9-11 LPD Web Page	86
Figure 9-12 LPD Configuration Web Page	87
Figure 10-1 SSH Server Host Keys Web Page	90
Figure 10-2 SSH Server Authorized Users Web Page	92
Figure 10-3 SSH Client Known Hosts Web Page	93

Figure 10-4 SSH Client Users Web Page	95
Figure 10-5 SSL Web Page	99
Figure 11-1 VIP Statistics Web Page	103
Figure 11-2 VIP Configuration Web Page	105
Figure 12-1 Filesystem Statistics Web Page	107
Figure 12-2 Filesystem Browser Web Page	108
Figure 12-3 TCP Web Page	110
Figure 12-4 IP Web Page	111
Figure 12-5 ICMP Web Page	112
Figure 12-6 ARP Web Page	113
Figure 12-7 IP Address Filter Web Page	114
Figure 12-8 Query Port Web Page	115
Figure 12-9 Diagnostics Hardware Web Page	116
Figure 12-10 MIB-II Network Statistics Web Page	117
Figure 12-11 IP Sockets Web Page	118
Figure 12-12 Ping Web Page	119
Figure 12-13 Traceroute Web Page	120
Figure 12-14 DNS Lookup Web Page	121
Figure 12-15 Memory Web Page	122
Figure 12-16 Buffer Pools Web Page	123
Figure 12-17 Processes Web Page	124
Figure 12-18 System Web Page	125
Figure 13-1 Email Statistics Web Page	127
Figure 13-2 Email 1 Configuration Web Page	128
Figure 13-3 CLI Statistics Web Page	130
Figure 13-4 CLI Configuration Web Page	131
Figure 13-5 XML Export Configuration Web Page	133
Figure 13-6 XML Export Status Web Page	134
Figure 13-7 Import Configuration Web Page	136
Figure 13-8 Import Configuration from External File Web Page	137
Figure 13-9 Import Configuration from Filesystem Web Page	138
Figure 13-10 Import Lines from Single Line Settings on the Filesystem Web Page	140
Figure 14-1 System Branding Web Page	143
Figure 15-1 System Web Page	144
Figure B-2 Scientific Calculator	147
Figure B-3 Hex Display	147

List of Tables

Table 1-1 Chapter/Appendix and Summary	12
Table 1-2 Conventions Used in This Book	13
Table 3-1 Current Settings and Description	21
Table 4-3 Summary of Web Manager Pages	26
Table 5-3 Network 1 Interface Configuration Fields	29
Table 5-5 Network 1 (eth0) Ethernet Link Fields	31
Table 6-1 Line 1 Configuration Fields	34
Table 6-2 Line 1 Command Mode Fields	36
Table 6-3 Tunnel 1 Serial Settings Fields	39
Table 6-4 Tunnel Packing Mode (Timeout) Fields	42
Table 6-5 Tunnel Packing Mode (Send Character) Fields	43
Table 6-6 Tunnel Accept Mode Fields	45
Table 6-7 Tunnel Connect Mode Fields	48
Table 6-8 Tunnel Disconnect Mode Fields	55
Table 6-9 Modem Emulation Commands and Descriptions	55
Table 6-10 Tunnel Modem Emulation Fields	57
Table 7-1 Terminal on Network Configuration Fields	60
Table 7-2 Terminal on Line 1 Configuration Fields	61
Table 7-3 Host Configuration Fields	63
Table 8-1 CPM CPs Current Configuration Fields and Descriptions	65
Table 8-2 CPM CPs Status Fields and Descriptions	66
Table 8-3 CPM Group Status Fields and Descriptions	67
Table 8-4 CPM Groups Current Configuration Fields and Descriptions	68
Table 9-1 PPP Configuration Fields	73
Table 9-2 SNMP Fields	74
Table 9-3 FTP Fields	76
Table 9-4 TFTP Server Fields	77
Table 9-5 Syslog Fields	79
Table 9-6 HTTP Configuration Fields	82
Table 9-7 HTTP Authentication Fields	83
Table 9-8 RSS Fields	85
Table 9-9 LPD Configuration Fields	87
Table 10-1 SSH Server Host Keys Fields	90
Table 10-2 SSH Server Authorized Users Fields	92
Table 10-3 SSH Client Known Hosts Fields	93
Table 10-4 SSH Client Users Fields	95
Table 10-5 Supported Cipher Suites	96
Table 10-6 SSL Fields	100
Table 11-1 VIP Statistics Fields	104
Table 12-1 Filesystem Browser Fields	109
Table 12-2 TCP Fields	110

Table 12-3 ARP Web Page Fields _____	113
Table 12-4 IP Address Filter Fields _____	114
Table 12-5 Ping Fields _____	119
Table 12-6 Traceroute Fields _____	120
Table 12-7 DNS Lookup Fields _____	122
Table 12-8 System Fields _____	125
Table 13-1 Email 1 Configuration Fields _____	129
Table 13-2 CLI Configuration Fields _____	131
Table 13-3 XML Export Configuration Fields _____	133
Table 13-4 XML Export Status Fields _____	135
Table 13-5 Import Configuration from Filesystem Fields _____	138
Table 13-6 Import Lines from Single Line Settings Fields _____	140
Table B-1 Conversion Values _____	146

1: About This Guide

This guide describes how to configure, use, and update the MatchPort AR. It is for software developers and original equipment manufacturers who are embedding the MatchPort AR in their designs. This chapter contains the following sections:

- ◆ [Chapter and Appendix Summaries](#)
- ◆ [Conventions](#)
- ◆ [Additional Documentation](#)

Chapter and Appendix Summaries

[Table 1-1](#) lists and summarizes each chapter and appendix.

Table 1-1 Chapter/Appendix and Summary

Chapter/Appendix	Summary
2: Overview	Main features of the product and the protocols it supports. Includes technical specifications.
3: Using DeviceInstaller	Instructions for viewing the current configuration using DeviceInstaller.
4: Configuration Using Web Manager	Instructions for accessing Web Manager and using it to configure settings for the MatchPort AR.
5: Network Settings	Instructions for using the web interface to configure Ethernet settings.
6: Line and Tunnel Settings	Instructions for using the web interface to configure lines and tunnels.
7: Terminal and Host Settings	Instructions for using the web interface to configure terminals and host settings.
8: Configurable Pins Manager	Instructions for using the Configurable Pins Manager (CPM) to set up the configurable pins to work with a device.
9: Services Settings	Instructions for using the web interface to configure settings for DNS, SNMP, FTP, and other services.
10: Security Settings	Description and configuration of SSH and SSL security settings and instructions for using the web interface to configure SSH and SSL security settings.
11: VIP	Information about Virtual IP (VIP) features available on the MatchPort AR and instructions for configuring a Virtual IP.
12: Maintenance and Diagnostics Settings	Instructions for using the web interface to maintain the MatchPort AR, view statistics, files, and logs, and diagnose problems.
13: Advanced Settings	Instructions for using the web interface to configure email, CLI, and XML settings.
14: Branding the MatchPort AR	Description of PPP on the MatchPort AR.

Table 1-1 Chapter/Appendix and Summary (continued)

Chapter/Appendix	Summary
15: Updating Firmware	Instructions for obtaining the latest firmware and updating the MatchPort AR.
A: Technical Support	Instructions for contacting Lantronix Technical Support.
B: Binary to Hexadecimal Conversions	Instructions for converting binary values to hexadecimal.
C: Compliance	Lantronix compliance information.

Conventions

Table 1-2 lists and describes the conventions used in this book.

Table 1-2 Conventions Used in This Book

Convention	Description
Bold text	Default parameters.
Brackets []	Optional parameters.
Angle Brackets < >	Possible values for parameters.
Pipe 	Choice of parameters.
Warning	Warning: Means that you are in a situation that could cause equipment damage or bodily injury. Before you work on any equipment, you must be aware of the hazards involved with electrical circuitry and familiar with standard practices for preventing accidents.
Note	Note: Means take notice. Notes contain helpful suggestions, information, or references to material not covered in the publication.
Caution	Caution: Means you might do something that could result in faulty equipment operation, or loss of data.
Screen Font (Courier New)	CLI terminal sessions and examples of CLI input.

Additional Documentation

Visit the Lantronix web site at www.lantronix.com/support/documentation for the latest documentation and the following additional documentation.

- ◆ **MatchPort AR Integration Guide**—Information about the MatchPort AR hardware, the MatchPort AR demonstration board, and integrating the MatchPort AR into your product.
- ◆ **MatchPort AR Command Reference**—Instructions for accessing Command Mode (the command line interface) using a Telnet connection or through the serial port. Detailed information about the commands. Also provides details for XML configuration and status.
- ◆ **MatchPort Demo Kit Quick Start**—Instructions for getting the MatchPort AR demonstration board up and running.

- ◆ **DeviceInstaller Online Help**—Instructions for using the Lantronix Windows-based utility to locate the MatchPort AR and to view its current settings.
- ◆ **Com Port Redirector Quick Start and Online Help**—Instructions for using the Lantronix Windows-based utility to create virtual com ports.
- ◆ **Secure Com Port Redirector User Guide**—Instructions for using the Lantronix Windows-based utility to create secure virtual com ports.

2: Overview

The MatchPort AR embedded Ethernet Device Server is a complete network-enabling solution on a 1.75" x 1.75" PCB. This miniature device server empowers original equipment manufacturers (OEMs) to go to market quickly and easily with Ethernet networking and web page serving capabilities built into their products.

This chapter contains the following sections:

- ◆ [Key Product Features](#)
- ◆ [Applications](#)
- ◆ [Protocol Support](#)
- ◆ [Evolution OS™](#)
- ◆ [Software Features](#)
- ◆ [Configuration Methods](#)
- ◆ [Addresses and Port Numbers](#)
- ◆ [Product Information Label](#)

Key Product Features

- ◆ **Power Supply:** Regulated 3.3V input required. There is a step-down converter to 1.5 volts for the processor core. All voltages have LC filtering to minimize noises and emissions.
- ◆ **Controller:** A Lantronix DSTni-FX 32-bit microprocessor, running at 166 MHz internal bus and 83 MHz external bus.
- ◆ **Memory:** 4 MB Flash and 8 MB SDRAM. Please contact your sales representative if you need larger memory sizes.
- ◆ **Ethernet:** 10/100 Mbps Ethernet transceiver (requires external magnetics and RJ45)
- ◆ **Serial Ports:** Two full, RS232-supporting serial ports with all hardware handshaking signals. Baud rates can be standard or customized up to 230 Kbps. Port 1 also supports RS422 and RS485.
- ◆ **Configurable IO Pins (CPs):** Up to seven pins are configurable as general purpose I/Os if no DTR or DCD is used on serial ports. Not 5V tolerant.
- ◆ **Interface Signals:** 3.3V-level interface signals.
- ◆ **Temperature Range:** Operates over an extended temperature range of -40°C to +85°C.

Applications

The MatchPort AR device server connects serial devices, such as those listed below to Ethernet networks using the IP protocol family:

- ◆ CNC controllers
- ◆ Data collection devices
- ◆ Universal Power Supply (UPS) management unit
- ◆ Telecommunications equipment

- ◆ Handheld instruments
- ◆ Security, alarm, and access control devices
- ◆ Patient monitoring equipment
- ◆ Medical instrumentation
- ◆ Industrial Manufacturing/Automation systems
- ◆ Building Automation equipment
- ◆ Point of Sale Systems
- ◆ ATM machines
- ◆ Data display devices
- ◆ Modems
- ◆ Time/attendance clocks and terminals

Protocol Support

The MatchPort AR device server supports the following TCP/IP protocols:

- ◆ ARP, IP, UDP, TCP, ICMP, BOOTP, DHCP, Auto IP, Telnet, DNS, FTP, TFTP, HTTP/HTTPS, SSH, SSL/TLS, SNMP, SMTP, RSS, PPP and Syslog for network communications and management.
- ◆ TCP, UDP, TCP/AES, UDP/AES, Telnet, SSH and SSL/TLS for tunneling to the serial port.
- ◆ TFTP, FTP, and HTTP for firmware upgrades and uploading files.

Evolution OS™

The MatchPort AR features the Lantronix 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
- ◆ Really Simple Syndication (RSS) information feeds
- ◆ Enterprise-grade security with SSL and SSH
- ◆ Comprehensive troubleshooting tools

Software Features

Modem Emulation

In modem emulation mode, the MatchPort AR can replace dial-up modems. The unit accepts modem AT commands on the serial port, and then establishes a network connection to the end device, leveraging network connections and bandwidth to eliminate dedicated modems and phone lines.

Web-Based Configuration and Troubleshooting

Built upon Internet-based standards, the MatchPort AR enables configuration, management, and troubleshooting by using a browser-based interface accessible anytime from anywhere. All configuration and troubleshooting options are available via the web interface. You can access all functions via a Web browser, for remote access. As a result, you decrease downtime (using the troubleshooting tools) and implement configuration changes (using the configuration tools).

Command-Line Interface (CLI)

Making the edge-to-enterprise vision a reality, the MatchPort AR with Evolution OS™ uses industry-standard tools for configuration, communication, and control. For example, the Evolution OS™ uses a Command Line Interface (CLI) whose syntax is very similar to that used by data center equipment such as routers and hubs.

VIP Access

Virtual IP Access is the Lantronix technology that solves the access-through-firewall problem. With VIP Access, the MatchPort AR can act as a ManageLinx DSC and provide direct access to your equipment behind a firewall.

SNMP Management

The MatchPort AR 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 MatchPort AR.

XML-Based Architecture and Device Control

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

Really Simple Syndication (RSS)

The MatchPort AR supports Really Simple Syndication (RSS) for streaming and managing on-line content. RSS feeds all the configuration changes that occur on the device. An RSS aggregator can be used to monitor many RSS feeds at one time. 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

Evolution OS™ provides the MatchPort AR the highest level of networking 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.

By protecting the privacy of serial data 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 or SSL connection.

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

You can use the MatchPort AR with the Lantronix 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.

Terminal Server/Device Management

Remote offices can have routers, PBXs, servers and other networking equipment that require remote management from the corporate facility. The MatchPort AR 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.

With the Login Connect Menu feature on the MatchPort AR, connections to the console ports of the attached devices as well as Ethernet hosts, such as Unix servers or another MatchPort AR, can easily be picked from a user-defined menu. This allows console ports across multiple devices to be accessed from one MatchPort AR.

Troubleshooting Capabilities

The MatchPort AR 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 MatchPort AR, including CPU utilization and total stack space available.

Configuration Methods

After installation, the MatchPort AR requires configuration. For the unit to operate correctly on a network, it must have a unique IP address on the network. There are four basic methods for logging into the MatchPort AR and assigning IP addresses and other configurable settings:

- ◆ **DeviceInstaller**—Configure the IP address and related settings and view current settings on the MatchPort AR using a PC GUI attached to a network. [See Using DeviceInstaller on page 21.](#)
- ◆ **Web Manager**—Use a web browser to configure the MatchPort AR settings using the Lantronix Web Manager. [See Configuration Using Web Manager on page 23.](#)
- ◆ **Command Line Interface (CLI)**—There are two methods for accessing CLI: making a Telnet connection or connecting a terminal (or a PC running a terminal emulation program) to the serial port. Refer to the *MatchPort AR Command Reference* for instructions and available commands.

- ◆ **XML**—The MatchPort AR supports XML-based configuration and setup records that make device configuration transparent to users and administrators. XML is easily editable with a standard text or XML editor. Refer to the *MatchPort AR Command Reference* for instructions and available commands.

Addresses and Port Numbers

Hardware Address

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

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

or

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

IP Address

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

Port Numbers

Every TCP connection and every UDP datagram is defined by a destination and source IP address, and a destination and source port number. For example, a Telnet server commonly uses port number 23.

The following is a list of the default server port numbers running on the MatchPort AR:

- ◆ TCP Port 22—SSH Server (Command Mode configuration)
- ◆ TCP Port 23—Telnet Server (Command Mode configuration)
- ◆ TCP Port 80—HTTP (Web Manager configuration)
- ◆ TCP Port 443—HTTPS (Web Manager configuration)
- ◆ UDP Port 161—SNMP
- ◆ TCP Port 21—FTP
- ◆ UDP Port 69—TFTP
- ◆ UDP Port 30718—LDP (Lantronix Discovery Protocol) port
- ◆ TCP/UDP Port 10001—Tunnel 1
- ◆ TCP/UDP Port 10002—Tunnel 2

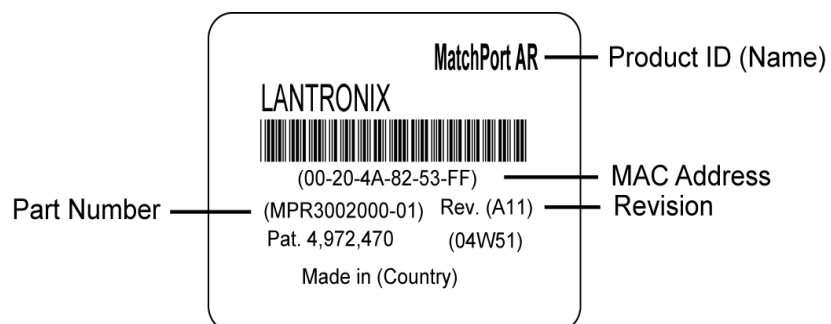
Product Information Label

Figure 2-1 shows the bottom of each unit which has a product information label. The label contains the following information:

- ◆ Product ID (name)
- ◆ Product description

- ◆ Bar code
- ◆ Part number
- ◆ Serial number (which is the hardware address, also referred to as Ethernet or MAC address)

Figure 2-1 MatchPort AR Product Information Label



3: Using DeviceInstaller

This chapter covers the steps for locating a MatchPort AR unit and viewing its properties and device details. It contains the following sections:

- ◆ [Accessing MatchPort AR using DeviceInstaller](#)
- ◆ [Device Details Summary](#)

DeviceInstaller is a free utility program provided by Lantronix that discovers, configures, upgrades, and manages Lantronix Device Servers. It can be downloaded from the Lantronix website at www.lantronix.com/support/downloads. For instructions on using DeviceInstaller to configure the IP address and related settings or for more advanced features, see the DeviceInstaller online Help.

Note: AutoIP generates a random IP address in the range of 169.254.0.1 to 169.254.255.254 if no BOOTP or DHCP server is found.

Accessing MatchPort AR using DeviceInstaller

Note: Keep a record of the MAC address because the MAC address is required to locate the MatchPort AR using DeviceInstaller.

1. Click **Start > All Programs > Lantronix > DeviceInstaller > DeviceInstaller**. When DeviceInstaller starts, it performs a network device search. To perform another search, click the Search button.
2. Expand the MatchPort folder by clicking the plus (+) symbol next to the folder icon. The list of available Lantronix MatchPort devices displays.
3. Select the MatchPort AR by expanding its entry and clicking on its hardware (MAC) address to view its configuration.
4. Click the **Device Details** tab, on the right. The current MatchPort AR configuration displays. This is only a subset of the complete configuration; access the complete configuration by using the Web Manager, CLI, or XML.

Device Details Summary

Table 3-1 lists and describes the display only settings unless otherwise noted.

Table 3-1 Current Settings and Description

Current Settings	Description
Name	Name identifying the MatchPort AR.
Group	Configurable field. Enter a group to categorize the MatchPort AR. Double-click the field, type in the value, and press Enter to complete. This group name is local to this PC and is not visible on other PCs or laptops using DeviceInstaller.
Comments	Configurable field. Enter comments for the MatchPort AR. Double-click the field, type in the value, and press Enter to complete. This description or comment is local to this PC and is not visible on other PCs or laptops using DeviceInstaller.

Table 3-1 Current Settings and Description (continued)

Current Settings	Description
Device Family	Shows the MatchPort AR device family type as "MatchPort".
Type	Shows the device type as MatchPort AR.
ID	Shows the MatchPort AR ID embedded within the unit.
Hardware Address	Shows the MatchPort AR hardware (MAC) address.
Firmware Version	Shows the firmware currently installed on the MatchPort AR.
Extended Firmware Version	Provides additional information on the firmware version.
Online Status	Shows the MatchPort AR status as Online, Offline, Unreachable (the MatchPort AR is on a different subnet), or Busy (the MatchPort AR is currently performing a task).
IP Address	Shows the MatchPort AR current IP address. To change the IP address, click the Assign IP button on the DeviceInstaller menu bar.
IP Address was Obtained	Displays dynamically if the MatchPort AR automatically received an IP address (e.g., from DHCP). Displays statically if the IP address was configured manually. If the IP address was assigned dynamically, the following fields appear: ◆ Obtain via DHCP with values of True or False. ◆ Obtain via BOOTP with values of True or False.
Subnet Mask	Shows the subnet mask specifying the network segment on which the MatchPort AR resides.
Gateway	Shows the IP address of the router of this network. There is no default.
Number of Ports	Shows the number of serial ports on this MatchPort AR.
Supports Configurable Pins	Shows True, indicating that configurable pins are available on the MatchPort AR.
Supports Email Triggers	Shows True, indicating email triggers are available on the MatchPort AR.
Telnet Enabled	Indicates whether Telnet is enabled on this MatchPort AR.
Telnet Port	Shows the MatchPort AR port for Telnet sessions.
Web Enabled	Indicates whether Web Manager access is enabled on this MatchPort AR.
Web Port	Shows the MatchPort AR port for Web Manager configuration.
Firmware Upgradeable	Shows True, indicating the MatchPort AR firmware is upgradeable as newer versions become available.

4: Configuration Using Web Manager

This chapter describes how to configure the MatchPort AR by using Web Manager, the Lantronix browser-based configuration tool. The configuration is stored in nonvolatile memory and is retained without power. All changes take effect immediately, unless otherwise noted. It contains the following sections:

- ◆ [Accessing Web Manager](#)
- ◆ [Web Manager](#)
- ◆ [Navigating the Web Manager](#)

Accessing Web Manager

Note: You can also access the Web Manager by selecting the Web Configuration tab on the DeviceInstaller window.

To access the Web Manager, perform the following steps.

1. Open a standard web browser. Lantronix supports the latest version of Internet Explorer, Mozilla Suite, Mozilla Firefox, Safari, or Opera.
2. Enter the IP address of the MatchPort AR in the address bar. The IP address may have been assigned manually using DeviceInstaller or the serial port (see the *MatchPort AR Demo Kit Quick Start Guide*) or automatically by DHCP.
3. Enter your username and password. The factory-default username is “admin” and the factory-default password is “PASS.” The Device Status web page shown in [Figure 4-1](#) displays configuration, network settings, line settings, tunneling settings, and product information.

The Home page is also the Device Status page which appears after you log into the Web Manager. It also appears when you click **Status** in the Main Menu.

Figure 4-1 MatchPort AR Web Manager Home Page

The screenshot displays the MatchPort AR Web Manager interface. The top header features the MatchPort AR ARCHITECT logo on the left and the LANTRONIX EVOLUTION OS™ logo on the right. A left-hand navigation menu lists various system functions: Status (highlighted with a home icon), CLI, CPM, Diagnostics, DNS, Email, Filesystem, FTP, Host, HTTP, IP Address Filter, Line, LPD, Network, PPP, Protocol Stack, Query Port, RSS, SNMP, SSH, SSL, Syslog, System, Terminal, TFTP, Tunnel, VIP, and XML. The main content area is titled "Device Status" and contains three tables: Product Information, Network Settings, and Line Settings. The Product Information table lists details such as Product Type, Firmware Version, Build Date, Serial Number, Uptime, and Permanent Config. The Network Settings table lists Interface, Link, MAC Address, Host, IP Address, Default Gateway, Domain, Primary DNS, and Secondary DNS. The Line Settings table lists Line 1 and Line 2 configurations. Below these tables is a Tunneling section with a table showing Connect Mode and Accept Mode for Tunnel 1 and Tunnel 2. The footer contains the copyright notice: Copyright © Lantronix, Inc. 2007-2010. All rights reserved.

Product Information		
Product Type:	Lantronix MatchPort AR	
Firmware Version:	5.1.0.0R10	
Build Date:	Mar 22 2010 (10:57:56)	
Serial Number:	77091427G6IM22	
Uptime:	6 days 21:36:10	
Permanent Config:	Saved	

Network Settings	
Interface:	eth0
Link:	Auto 10/100 Mbps Auto Half/Full (100 Mbps Half)
MAC Address:	00:20:4a:a7:06:2a
Host:	<None>
IP Address:	172.19.205.59 / 255.255.0.0
Default Gateway:	172.19.0.1
Domain:	<None>
Primary DNS:	172.19.1.1
Secondary DNS:	<None>

Line Settings		
Line 1:	RS232, 9600, None, 8, 1, Hardware	
Line 2:	RS232, 9600, None, 8, 1, None	

Tunneling	Connect Mode	Accept Mode
Tunnel 1:	Disabled	Waiting
Tunnel 2:	Disabled	Waiting

Copyright © Lantronix, Inc. 2007-2010. All rights reserved.

Web Manager

Figure 4-2 shows the components of a typical Web Manager page.

Figure 4-2 Components of a Typical Web Manager Page

The screenshot displays the MatchPort AR web manager interface. The header shows the MatchPort AR logo and Lantronix Evolution OS. The left menu bar lists various configuration options. The main content area displays the 'Device Status' page, which includes product information and network settings. The footer contains copyright information for Lantronix, Inc. Annotations indicate the Header, Menu Bar, Configuration & Status Area, and a Help area on the right.

Product Information	
Product Type:	Lantronix MatchPort AR
Firmware Version:	5.1.0.0R10
Build Date:	Mar 22 2010 (10:57:56)
Serial Number:	77091427G6IM22
Uptime:	6 days 21:36:10
Permanent Config:	Saved

Network Settings	
Interface:	eth0
Link:	Auto 10/100 Mbps Auto Half/Full (100 Mbps Half)
MAC Address:	00:20:4a:a7:06:2a
Host:	<None>
IP Address:	172.19.205.59 / 255.255.0.0
Default Gateway:	172.19.0.1
Domain:	<None>
Primary DNS:	172.19.1.1
Secondary DNS:	<None>

Line Settings	
Line 1:	RS232, 9600, None, 8, 1, Hardware
Line 2:	RS232, 9600, None, 8, 1, None

Tunneling	Connect Mode	Accept Mode
Tunnel 1:	Disabled	Waiting
Tunnel 2:	Disabled	Waiting

The Menu Bar (orange) always appears at the left side of the web page. There are accessible sections listed in the Main Menu, such as CLI, Diagnostics, Protocol Stack, etc. To display one of these sections, click it.

The Help displays on the right side of the web page and contains information or instructions associated with the page.

The center of a web page contains the following additional sections:

- ◆ At the top, there are links to configurable fields. The links often indicate the configurable field, for example, Line, Host, or Tunnel.
- ◆ In the middle, you can select or enter new configuration settings. Some pages display statistics or status in this area rather than allow you to enter settings.
- ◆ At the bottom, the current configuration displays. In some cases, you can reset or clear a setting.
- ◆ At the very bottom, the copyright information displays with a link to the Lantronix home page.

Navigating the Web Manager

The Web Manager provides an intuitive point-and-click interface. A menu bar on 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 MatchPort AR for the new configuration settings to take effect. The chapters that follow indicate when a change requires a reboot.*

Table 4-3 Summary of Web Manager Pages

Web Manager Page	Description	Page
Status	Shows product information and network, line, and tunneling settings.	24
CLI	Shows Command Line Interface (CLI) statistics and lets you change the current CLI configuration settings.	129
CPM	Shows information about the Configurable Pins Manager (CPM) and how to set the configurable pins and pin groups to work with a device.	64
Diagnostics	Lets you perform various diagnostic procedures.	106
DNS	Shows the current configuration of the DNS subsystem and the DNS cache.	71
Email	Shows email statistics and lets you clear the email log, configure email settings, and send an email.	127
Filesystem	Shows file system statistics and lets you browse the file system to view a file, create a file or directory, upload files using HTTP, copy a file, move a file, or perform TFTP actions.	107
FTP	Shows statistics and lets you change the current configuration for the File Transfer Protocol (FTP) server.	76
Host	Lets you view and change settings for a host on the network.	62
HTTP	Shows HyperText Transfer Protocol (HTTP) statistics and lets you change the current configuration and authentication settings.	80
IP Address Filter	Lets you specify all the IP addresses and subnets that are allowed to send data to this device.	114
Line	Shows statistics and lets you change the current configuration and Command mode settings of a serial line.	32
LPD	Shows LPD (Line Printer Daemon) Queue statistics and lets you configure the LPD and print a test page.	86
Network	Shows status and lets you configure the network interface.	29
PPP	Lets you configure a network link using Point-to-Point Protocol (PPP) over a serial line.	72
Protocol Stack	Lets you perform lower level network stack-specific activities.	110
Query Port	Lets you change configuration settings for the query port.	115

Table 4-3 Summary of Web Manager Pages (continued)

Web Manager Page	Description	Page
RSS	Lets you change current Really Simple Syndication (RSS) settings.	85
SNMP	Lets you change the current Simple Network Management Protocol (SNMP) configuration settings.	74
SSH	Lets you change the configuration settings for SSH server host keys, SSH server authorized users, SSH client known hosts, and SSH client users.	90
SSL	Lets you upload an existing certificate or create a new self-signed certificate.	99
Syslog	Lets you specify the severity of events to log and the server and ports to which the syslog should be sent.	78
System	Lets you reboot the MatchPort AR, restore factory defaults, upload new firmware, and change the MatchPort AR long and short names.	125
Terminal	Lets you change current settings for a terminal.	59
TFTP	Shows statistics and lets you change the current configuration for the Trivial File Transfer Protocol (TFTP) server.	77
Tunnel	Lets you change the current configuration settings for a tunnel.	37
VIP	Lets you configure Virtual IP addresses to be used in Tunnel Accept Mode and Tunnel Connect Mode.	102
XML	Lets you export XML configuration and status records, and import XML configuration records.	132

5: Network Settings

This chapter describes how to access, view, and configure network settings from the Network web page. The **Network** web page contains sub-menus that enable you to view and configure the aspects of your network.

This chapter contains the following sections:

- ◆ [Network 1 Interface Status](#)
- ◆ [Network 1 Interface Configuration](#)
- ◆ [Network 1 Ethernet Link](#)

Network 1 Interface Status

To view the Network 1 interface status, click Network on the Main Menu. [Figure 5-1](#) shows the page that displays. Using this page, you can view the status on your network interfaces.

Figure 5-1 Network1 (eth0) Interface Status Web Page

Network 1

InterfaceLink

StatusConfiguration

Network 1 (eth0) Interface Status

	Current	After Reboot
BOOTP Client:	Off	Off
DHCP Client:	On [Renew]	On
IP Address:	172.19.100.220 (DHCP)	<DHCP>
Network Mask:	255.255.0.0 (DHCP)	<DHCP>
Default Gateway:	172.19.0.1 (DHCP)	<DHCP>
Hostname:	<None>	<DHCP>
Domain:	eng.lantronix.com (DHCP)	<DHCP>
DNS Suffix Search List:	eng.lantronix.com. int.lantronix.com. lantronix.com.	<DHCP>
DHCP Client ID:	<None>	<None>

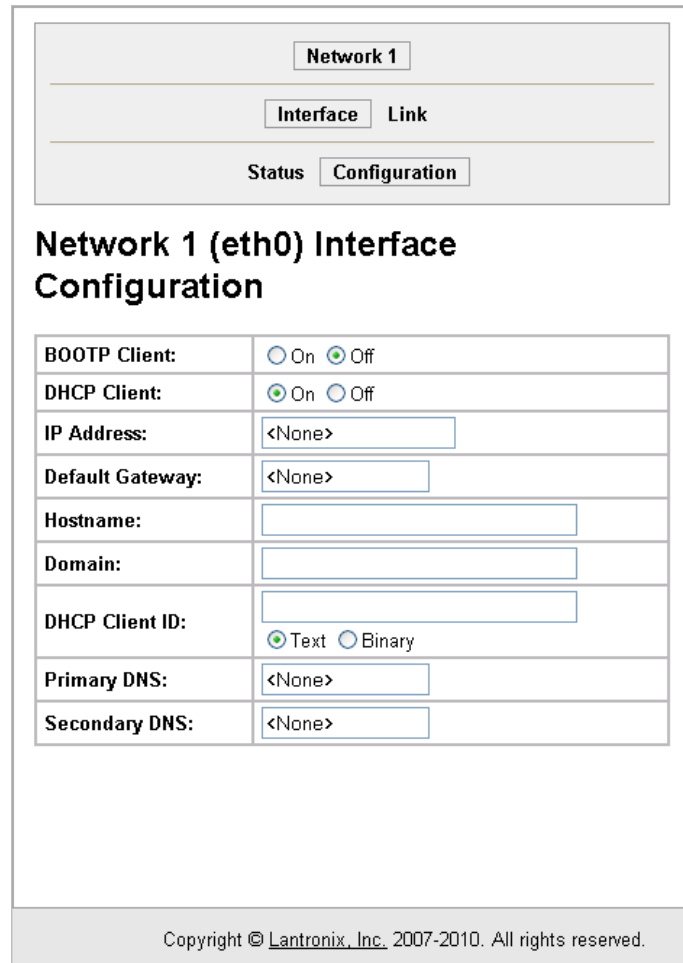
Copyright © Lantronix, Inc. 2007-2010. All rights reserved.

Network 1 Interface Configuration

To configure the Network interface, perform the following steps.

1. Click **Network** on the Main Menu.
2. Click **Network 1 > Interface > Configuration**. [Figure 5-2](#) shows the page that displays.

Figure 5-2 Network 1 (eth0) Interface Configuration Web Page



Network 1

Interface Link

Status Configuration

Network 1 (eth0) Interface Configuration

BOOTP Client:	☐ On ☒ Off
DHCP Client:	☒ On ☐ Off
IP Address:	<None>
Default Gateway:	<None>
Hostname:	
Domain:	
DHCP Client ID:	☒ Text ☐ Binary
Primary DNS:	<None>
Secondary DNS:	<None>

Copyright © Lantronix, Inc. 2007-2010. All rights reserved.

3. Enter or modify the fields in [Table 5-3](#).

Table 5-3 Network 1 Interface Configuration Fields

Field	Description
BOOTP Client	Select On or Off. At boot up the MatchPort AR will attempt to obtain an IP address from a BOOTP server. Notes: ◆ Overrides the configured IP address, network mask, gateway, hostname, and domain. ◆ When DHCP is On, the system automatically uses DHCP, regardless of whether BOOTP Client is On.

Table 5-3 Network 1 Interface Configuration Fields (continued)

Field	Description
DHCP Client	Select On or Off . At boot up the MatchPort AR will attempt to lease an IP address from a DHCP server and maintain the lease at regular intervals. Note: Overrides BOOTP, the configured IP address, network mask, gateway, hostname, and domain.
IP Address	Enter the MatchPort AR static IP address. You may enter it alone, in CIDR format, or with an explicit mask. The IP address is used if BOOTP and DHCP are both set to Off . Changing this value requires you to reboot the MatchPort AR. Note: When DHCP is enabled, the MatchPort AR tries to obtain an IP address from DHCP. If it cannot, AutoIP, a server-less method of selecting the IP address when the DHCP server is unavailable, assigns an address in the range of 169.254.xxx.xxx.
Default Gateway	Enter the IP address of the router for this network. Or clear the field (appears as <None>). This address is only used for static IP address configuration.
Hostname	Enter the MatchPort AR hostname. It must begin with a letter, continue with a sequence of letters, numbers, and/or hyphens, and end with a letter or number.
Domain	Enter the domain name.
DHCP Client ID	Enter the ID if the DHCP server uses a DHCP ID. The DHCP server lease table shows IP addresses and MAC addresses for devices. The lease table shows the Client ID, in hexadecimal notation, instead of the MatchPort AR MAC address.
Primary DNS	IP address of the primary name server. This entry is required if you choose to configure a DNS (Domain Name Server).
Secondary DNS	IP address of the secondary DNS.

4. Click **Submit**. Changes to the following settings require a reboot for the changes to take effect:
 - ◆ BOOTP Client
 - ◆ DHCP Client
 - ◆ IP address
 - ◆ DHCP Client ID

Network 1 Ethernet Link

To display and change settings in the Network 1 Ethernet Link web page, perform the following steps.

1. Click **Network** on the Main Menu.

2. Click **Network 1 > Link**. [Figure 5-4](#) shows the page that displays.

Figure 5-4 Network1 (eth0) Ethernet Link Web Page

Network 1

InterfaceLink

Network 1 (eth0) Ethernet Link

Status

Speed:	100 Mbps
Duplex:	Half

Configuration

Speed:	☒ Auto ☐ 10Mbps ☐ 100Mbps
Duplex:	☒ Auto ☐ Half

Copyright © Lantronix, Inc. 2007-2010. All rights reserved.

3. Enter or modify the fields in [Table 5-5](#).

Table 5-5 Network 1 (eth0) Ethernet Link Fields

Field	Description
Speed	Select the Ethernet link speed. Auto is the default.
Duplex	Select the Ethernet link duplex mode. Auto is the default.

4. Click **Submit**.

6: Line and Tunnel Settings

This chapter describes how to view and configure lines and tunnels. It contains the following sections:

- ◆ [Line Settings](#)
- ◆ [Tunnel Settings](#)

Line Settings

You can view statistics and configure the serial interfaces (referred to as lines) by using the **Line** web page. When you click **Line** from the Main Menu, **Line 1** fields display. To go to **Line 2**, click the **Line 2** button.

The following sub-menus you can use:

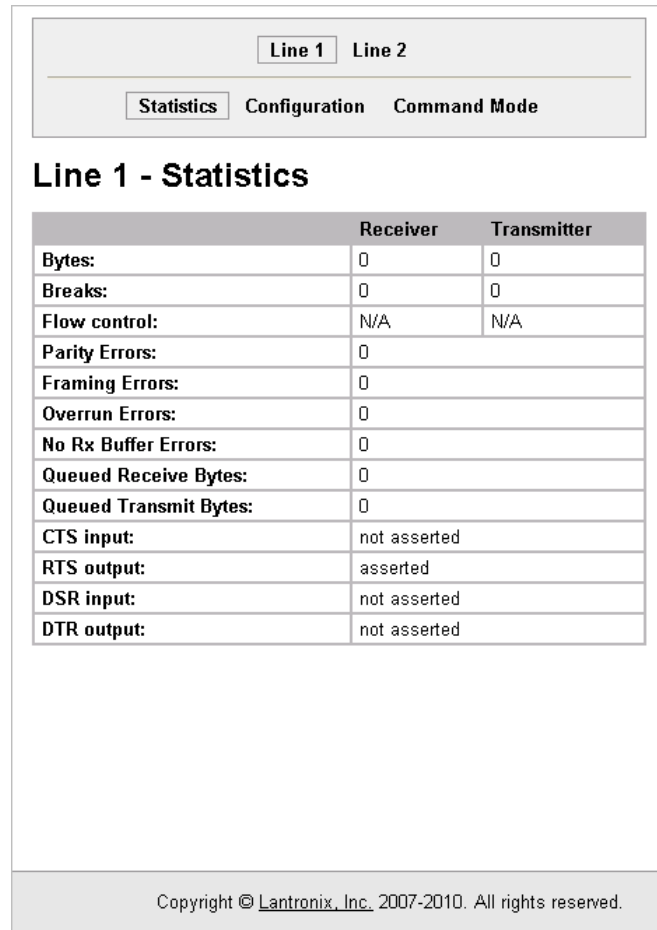
- ◆ **Line Statistics**—Displays statistics for the two lines. For example, the bytes received and transmitted, breaks, flow control, parity errors, etc.
- ◆ **Line Configuration**—Enables the change of the name, interface, protocol, baud rates, and parity, etc.
- ◆ **Line Command Mode**—Enables the types of modes, wait time, serial strings, signon message, etc.

Line Statistics

To display the line statistics, perform the following steps.

1. Click **Line** on the Main Menu. [Figure 6-1](#) shows the page that displays.

Figure 6-1 Line 1 Statistics Web Page



Line Configuration

To configure a line, perform the following steps.

1. Click **Line > Line 1 > Configuration**. Line 2 has the same fields as Line 1. [Figure 6-2](#) shows the page that displays.

Figure 6-2 Line 1 Configuration Web Page

Line 1
Line 2

Statistics
Configuration
Command Mode

Line 1 - Configuration

Configuration	Status
Name:	
Interface: RS232 ▼	
State: Enabled ▼	Enabled
Protocol: Tunnel ▼	Tunnel
Baud Rate: 9600 ▼	9600
Parity: None ▼	None
Data Bits: 8 ▼	8
Stop Bits: 1 ▼	1
Flow Control: None ▼	None
Xon Char: <control>Q	<control>Q
Xoff Char: <control>S	<control>S
Gap Timer: <None> milliseconds	
Threshold: 56 bytes	

Copyright © Lantronix, Inc. 2007-2010. All rights reserved.

2. Enter or modify the fields in [Table 6-1](#).

Table 6-1 Line 1 Configuration Fields

Field	Description
Name	Enter a name for the line.
Interface	Select the interface type from the drop-down menu. The default is RS232.
State	Indicates whether the current line is enabled. To change the status, select Enabled or Disabled from the drop-down menu.
Protocol	Select the protocol from the drop-down menu. The default is Tunnel. Note: All protocols work in Connect and Accept Mode except the LPD or Tunnel protocol option which is supported only in Accept Mode .
Baud Rate	Select the baud rate from the drop-down menu. The default is 9600.
Parity	Select the parity from the drop-down menu. The default is None.
Data Bits	Select the number of data bits from the drop-down menu. The default is 8.

Table 6-1 Line 1 Configuration Fields (continued)

Field	Description
Stop Bits	Select the number of stop bits from the drop-down menu. The default is 1.
Flow Control	Select the flow control from the drop-down menu. The default is None.
Xon Char	Specify the character to use to start the flow of data when Flow Control is set to Software. 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	Specify the character to use to stop the flow of data when Flow Control is set to Software. Prefix a decimal character with \ or a hexadecimal character with 0x, or provide a single printable character. The default Xoff char is 0x13.
Gap Timer	The driver forwards received serial bytes after the Gap Timer delay from the last character received. By default, the delay is four character periods at the current baud rate (minimum 1 ms).
Threshold	The driver will also forward received characters after Threshold bytes have been received.

3. Click **Submit**.

Line Command Mode

To configure the Command Mode, perform the following steps.

1. Click **Line > Line 1 > Command Mode**. [Figure 6-3](#) shows the page that displays.

Figure 6-3 Line 1 Command Mode Web Page

Line 1 - Command Mode

Mode: ☐ Always ☐ Use Serial String ☐ Use CP Group ☐ Use both Serial String and CP Group ☐ Disabled

Wait Time: milliseconds

Serial String: ☒ Text ☐ Binary

Echo Serial String: ☐ Yes ☐ No

CP Group: Group: Value:

Signon Message: ☒ Text ☐ Binary

Current Configuration

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

Copyright © Lantronix, Inc. 2007-2010. All rights reserved.

2. Enter or modify the fields in [Table 6-2](#).

Table 6-2 Line 1 Command Mode Fields

Field	Description
Mode	Select the method of enabling Command Mode or choose to disable Command Mode. ◆ Always—Immediately enables Command Mode for the serial line. ◆ Use Serial String—Enables Command Mode when the serial string is read on the serial line during boot time. ◆ Use CP Group—Enables Command Mode based on the status of a CP Group. ◆ Use both Serial String and CP Group—Enables Command Mode when both the serial string and the value of the CP Group are matched. ◆ Disabled—Turns off Command Mode.
Wait Time	Enter the wait time for the serial string during boot-up in milliseconds.

Table 6-2 Line 1 Command Mode Fields (continued)

Field	Description
Serial String	Enter the serial string characters. Select a string type. ◆ Text—String of bytes that must be read on the Serial Line during boot time to enable Command Mode. It may contain a time element in x milliseconds, in the format {x}, to specify a required delay. ◆ Binary—String of characters representing byte values where each hexadecimal byte value starts with \0x and each decimal byte value starts with backslash (\).
Echo Serial String	Select Yes to enable echoing of the serial string at boot-up.
CP Group	Enter the CP Group name and value after selecting Use CP Group in the Mode field. When the value matches the current value of the group, Command Mode is enabled on the Serial Line.
Signon Message	Enter the boot-up signon message. Select a string type. ◆ Text—String of bytes sent on the serial line during boot time. ◆ Binary—One or more byte values separated by commas. Each byte value may be decimal or hexadecimal. Start hexadecimal values with 0x. Note: This string gets output on the serial port at boot, regardless of whether command mode is enabled or not.

3. Click **Submit**.

Tunnel Settings

Tunneling allows serial devices to communicate over a network, without “being aware” of the devices which establish the network connection between them. When any character is transmitted to the serial port, it gets copied to the network connection. Tunneling parameters are configured using the Web Manager (see [Tunnel Settings on page 37](#)) or CLI Tunnel Menu (refer to the *MatchPort AR Command Reference*) for the full list of commands.)

The MatchPort AR supports two connections simultaneously per serial port. One of the connections is Connect Mode and the other connection is Accept Mode. The connections on one serial port are separate from those on the other serial port.

- ◆ **Connect Mode**—Makes an active connection. The receiving node on the network must listen for the Connect Mode connection. Connect Mode is disabled by default.
- ◆ **Accept Mode**—Listens for a connection. A node on the network initiates the connection. Accept Mode is enabled by default.
- ◆ **Disconnect Mode**—Defines how an open connection stops the forwarding of data. The specific parameters to stop the connection are configurable. Once a defined event occurs, the MatchPort AR disconnects Accept Mode and Connect Mode connections on that port.

You can view statistics and configure two tunnels by using the **Tunnel** web page. When you click **Tunnel** from the Main Menu, Tunnel 1 fields display. To go to Tunnel 2, click the Tunnel 2 button. There are six sub-menus that you can use as follows:

- ◆ **Statistics**—Displays statistics for the two lines. For example, completed accepts, completed connects, disconnects, dropped accepts, dropped connects, etc.
- ◆ **Serial Settings**—Configures buffer size and DTR.

- ◆ **Connect Mode**—Controls how a tunnel behaves when a connection attempt originates locally.
- ◆ **Accept Mode**—Controls how a tunnel behaves when a connection attempt originates from the network.
- ◆ **Disconnect Mode**—Relates to the disconnect of a tunnel.
- ◆ **Packing Mode**—Sends packed data that is queued in larger chunks instead of sending it immediately after being read on the serial line.
- ◆ **Modem Emulation**—Initiates and accepts tunnel connections using the AT commands.

Tunnel Statistics

The MatchPort AR logs tunneling statistics. The **Dropped** statistic shows connections ended by the remote location. The **Disconnects** statistic shows connections ended by the MatchPort AR.

To display the tunnel statistics, perform the following steps.

1. Click **Tunnel** on the **Main Menu**. [Figure 6-4](#) shows the page that displays.

Figure 6-4 Tunnel 1 Statistics Web Page

Tunnel 1 Tunnel 2	
Statistics	Serial Settings Packing Mode
Accept Mode	Connect Mode Disconnect Mode
	Modem Emulation

Tunnel 1- Statistics

Aggregate Counters	
Completed Accepts:	0
Completed Connects:	0
Disconnects:	0
Dropped Accepts:	0
Dropped Connects:	0
Octets forwarded from Serial:	0
Octets forwarded from Network:	0
Accept Connection Time:	0 days 00:00:00
Connect 1 Connection Time:	0 days 00:00:00
Connect 2 Connection Time:	0 days 00:00:00
Connect 3 Connection Time:	0 days 00:00:00
Connect 4 Connection Time:	0 days 00:00:00
Connect 5 Connection Time:	0 days 00:00:00
Connect 6 Connection Time:	0 days 00:00:00
Connect 7 Connection Time:	0 days 00:00:00
Connect 8 Connection Time:	0 days 00:00:00
Connect 9 Connection Time:	0 days 00:00:00
Connect 10 Connection Time:	0 days 00:00:00
Connect 11 Connection Time:	0 days 00:00:00

Serial Settings

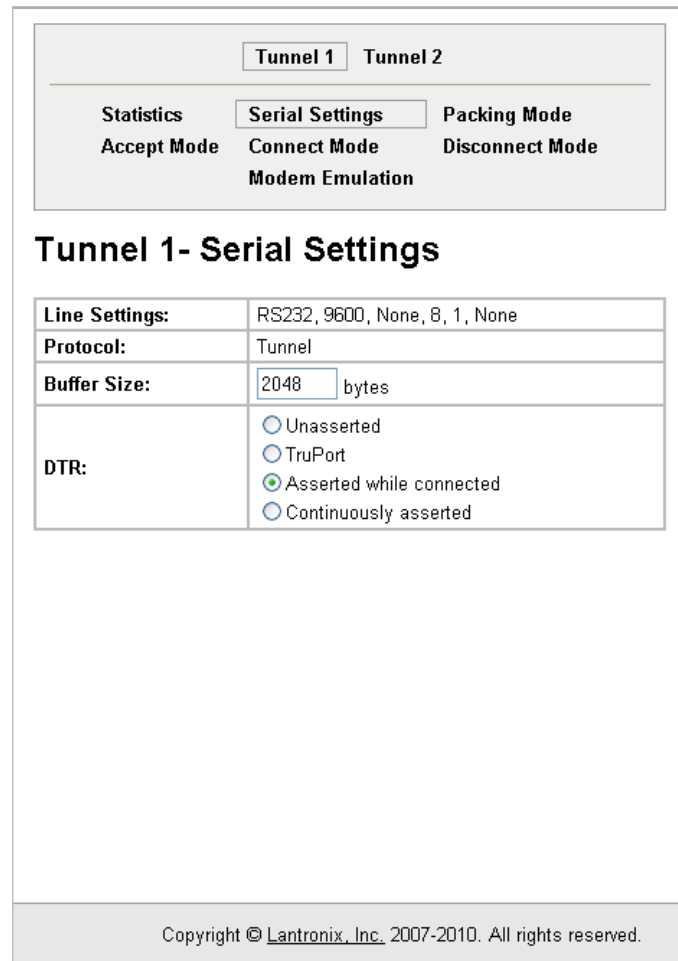
Serial line settings are configurable for both serial line 1 and serial line 2. Configure the buffer size to change the maximum amount of data the serial port stores. For any active connection, the MatchPort AR sends the data in the buffer.

The modem control signal DTR on the Line may be continually asserted or asserted only while either an Accept Mode tunnel or a Connect Mode tunnel is connected.

To configure the serial settings, perform the following steps.

1. Click **Tunnel > Tunnel 1 > Serial Settings**. [Figure 6-5](#) shows the page that displays.

Figure 6-5 Tunnel 1 Serial Settings Web Page



Tunnel 1
Tunnel 2

Statistics
Serial Settings
Packing Mode

Accept Mode
Connect Mode
Disconnect Mode

Modem Emulation

Tunnel 1- Serial Settings

Line Settings:	RS232, 9600, None, 8, 1, None
Protocol:	Tunnel
Buffer Size:	2048 bytes
DTR:	☐ Unasserted ☐ TruPort ☒ Asserted while connected ☐ Continuously asserted

Copyright © Lantronix, Inc. 2007-2010. All rights reserved.

2. View or modify the fields in [Table 6-3](#).

Table 6-3 Tunnel 1 Serial Settings Fields

Fields	Description
Line Settings	Display only field. Current serial settings for the line.
Protocol	Display only field. The protocol being used for the tunnel.
Buffer Size	Enter the buffer size used for the tunneling of serial data received. Requires reboot to take effect.

Table 6-3 Tunnel 1 Serial Settings Fields (continued)

Fields	Description
DTR	Select when to assert DTR. ◆ Unasserted ◆ TruPort—Asserted whenever a connect mode or an accept mode tunnel connection is active with the Telnet Protocol RFC2217. The remote DSR is asserted. ◆ Asserted while connected—Asserted whenever a connect or an accept mode tunnel connection is active. ◆ Continuously asserted—Asserted regardless of the status of a tunnel connection. Status of a tunnel connection does not affect the DTR signal.

3. Click **Submit**.

Packing Mode

Packing Mode takes data from the serial port, packs it together, and sends over the network. Packing can be configured based on threshold (size in bytes, timeout (milliseconds), or a single character.

Size is set by modifying the threshold field. When the number of bytes reaches the threshold, a packet is sent immediately.

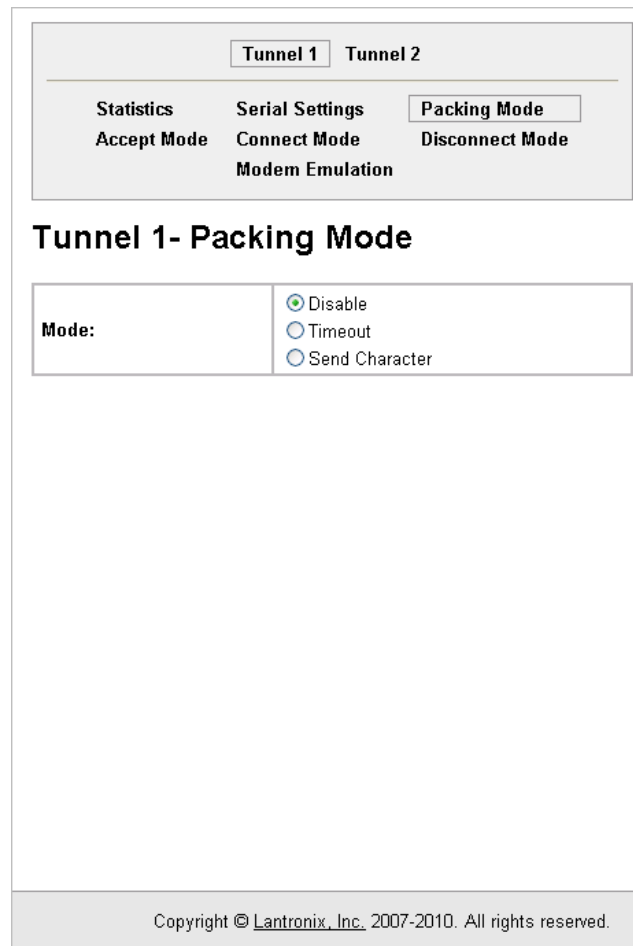
The timeout field is used to force a packet to be sent after a maximum time. The packet is sent even if the threshold value is not reached.

When Send Character is configured, a single printable character or control character read on the Serial Line forces the packet to be sent immediately. There is an optional trailing character parameter which can be specified. It can be a single printable character or a control character.

To configure the tunnel packing mode, perform the following steps.

1. Click **Tunnel > Tunnel 1 > Packing Mode**. [Figure 6-6](#) shows the page that displays.

Figure 6-6 Tunnel 1 Packing Mode Web Page



Tunnel 1 Tunnel 2	
Statistics	Serial Settings
Accept Mode	Connect Mode
	Disconnect Mode
	Modem Emulation

Tunnel 1- Packing Mode

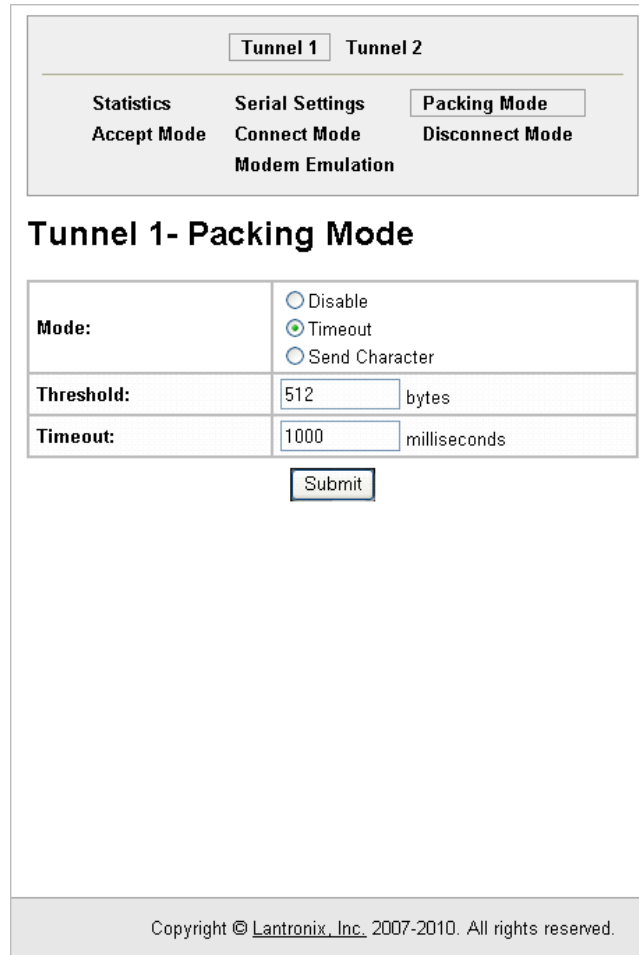
Mode:	☒ Disable ☐ Timeout ☐ Send Character
--------------	---

Copyright © Lantronix, Inc. 2007-2010. All rights reserved.

Packing Mode using Timeout

To configure Packing Mode using Timeout, click **Timeout**. Figure 6-7 shows the page that displays.

Figure 6-7 Tunnel 1 Packing Mode (Timeout)



Tunnel 1 Tunnel 2

Statistics Serial Settings **Packing Mode**
Accept Mode Connect Mode Disconnect Mode
Modem Emulation

Tunnel 1- Packing Mode

Mode:	☐ Disable ☒ Timeout ☐ Send Character	
Threshold:	512	bytes
Timeout:	1000	milliseconds

Submit

Copyright © Lantronix, Inc., 2007-2010. All rights reserved.

1. Enter or modify the fields in Table 6-4.

Table 6-4 Tunnel Packing Mode (Timeout) Fields

Field	Description
Threshold	Send the queued data when the number of queued bytes reaches the threshold value.
Timeout	Enter a time, in milliseconds, for the MatchPort AR to send the queued data after the first character was received.

2. Click **Submit**.

Packing Mode using Send Character

To configure Packing Mode using Send Character, click **Send Character**. Figure 6-8 shows the page that displays.

Figure 6-8 Tunnel 1 Packing Mode (Send Character)

Tunnel 1
Tunnel 2

Statistics
 Accept Mode

Serial Settings
 Connect Mode
 Modem Emulation

Packing Mode
 Disconnect Mode

Tunnel 1- Packing Mode

Mode:	☐ Disable ☐ Timeout ☒ Send Character
Threshold:	512 bytes
Send Character:	⟨control⟩M
Trailing Character:	⟨None⟩

Copyright © Lantronix, Inc. 2007-2010. All rights reserved.

1. Enter or modify the fields in Table 6-5.

Table 6-5 Tunnel Packing Mode (Send Character) Fields

Field	Description
Threshold	Send the queued data when the number of queued bytes reaches the threshold value.
Send Character	Enter a single character, either a printable character or control character, for the send character. Upon receiving this character on the serial line, the MatchPort AR sends out the queued data.
Trailing Character	This is an optional setting. Enter a single character, either a printable character or control character, for the trailing character. This character is sent immediately following the send character.

2. Click **Submit**.

Accept Mode

In Accept Mode, the MatchPort AR waits for a connection from the network. 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 and 10002 for serial port 2.

Accept Mode supports the following protocols:

- ◆ SSH (MatchPort AR acts as the server). When using SSH, the SSH server host keys and at least one SSH authorized user must be configured.
- ◆ SSL
- ◆ TCP
- ◆ AES encryption over TCP
- ◆ Telnet (MatchPort AR supports IAC codes. It drops the IAC codes when Telnetting and does not forward them to the serial port).

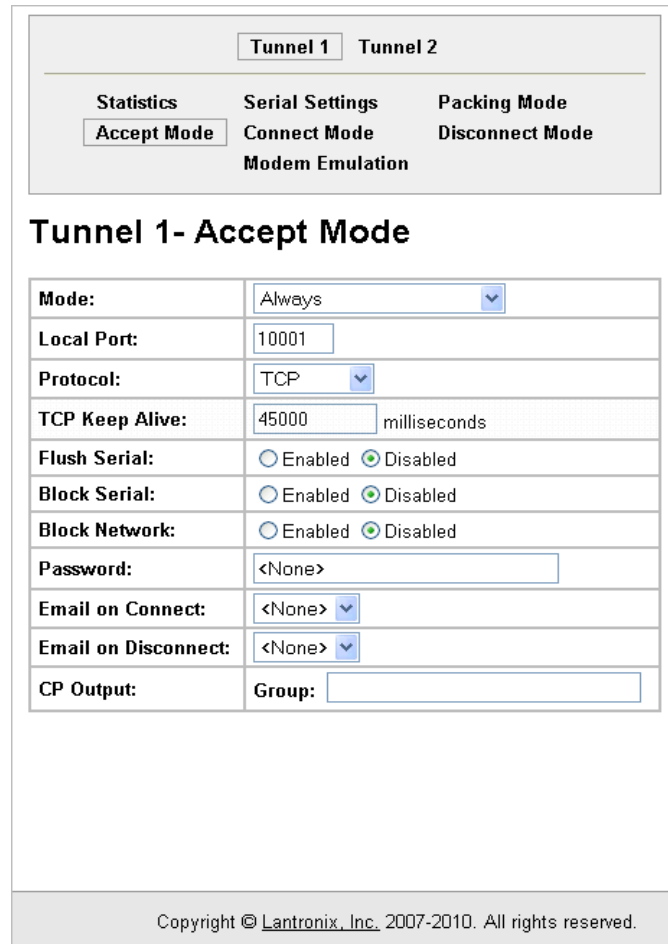
Accept Mode has the following states:

- ◆ Disabled (never a 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
- ◆ Modem emulation

To configure Accept Mode, perform the following steps.

1. Click **Tunnel 1 > Accept Mode**. Figure 6-9 shows the page displays.

Figure 6-9 Tunnel 1 Accept Mode Web Page



2. Enter or modify the fields in Table 6-6.

Table 6-6 Tunnel Accept Mode Fields

Field	Description
Mode	Select the method used to start a tunnel in Accept mode. Choices are: ◆ Disabled—Do not accept an incoming connection. ◆ Always—Accept an incoming connection. (<i>default</i>) ◆ Any Character—Start waiting for an incoming connection when any character is read on the serial line. ◆ Start Character—Start waiting for an incoming connection when the start character for the selected tunnel is read on the serial line. ◆ Modem Control Asserted—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. ◆ Modem Emulation—Start waiting for an incoming connection when triggered by modem emulation AT commands. Connect mode must also be set to Modem Emulation.

Table 6-6 Tunnel Accept Mode Fields (continued)

Field	Description
Local Port	Enter the port number for use as the local port. The defaults are port 10001 for Tunnel 1 and port 10002 for Tunnel 2.
Protocol	Select the protocol type for use with Accept Mode. The default protocol is TCP. If you select TCP AES you will need to configure the AES keys.
TCP Keep Alive	Enter the time, in seconds, the MatchPort AR waits during a silent connection before checking if the currently connected network device is still on the network. If the unit then gets no response after 8 attempts, it drops that connection.
Flush Serial Data	Select Enabled to flush the serial data buffer on a new connection.
Block Serial Data	Select On to block, or not tunnel, serial data transmitted to the MatchPort AR.
Block Network Data	Select On to block, or not tunnel, network data transmitted to the MatchPort AR.
Password	Enter a password that clients must send to the MatchPort AR 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 MatchPort AR must be terminated with one of the following: (a) 0x0A (LF), (b) 0x00, (c) 0x0D 0x0A (CR LF), or (d) 0x0D 0x00.
Email on Connect	Select whether the MatchPort AR sends an email when a connection is made. Select None if you do not want to send an email. Otherwise, select the Email profile to use for sending.
Email on Disconnect	Select whether the MatchPort AR sends an email when a connection is closed. Select None if you do not want to send an email. Otherwise, select the Email profile to use for sending.
CP Output	Enter a CP Group whose value should change when a connection is established and dropped. ◆ Connection value—Specifies the value to set the CP Group to when a connection is established. ◆ Disconnection value—Specifies the value to set the CP Group to when the connection is closed.

3. Click **Submit**.

Connect Mode

Connect Mode defines how the MatchPort AR makes an outgoing connection. For Connect Mode to function, it must be enabled, have a remote station configured, and a remote port configured (TCP or UDP). When enabled, Connect Mode is always on.

Enter the remote station as an IP address or DNS name. The MatchPort AR will not make a connection unless it can resolve the address. For DNS names, after 4 hours of an active connection, the MatchPort AR will re-evaluate the address. If it is a different address, it will close the connection.

Connect Mode supports the following protocols:

- ◆ TCP
- ◆ AES encryption over TCP and UDP
- ◆ SSH (the MatchPort AR is the SSH client)
- ◆ SSL
- ◆ UDP (available only in Connect Mode because it is a connectionless protocol).
- ◆ Telnet

Note: *The Local Port in Connect Mode is independent of the port configured in Accept Mode.*

Connect Mode has six modes used to initiate and maintain a connection:

- ◆ Disabled (no connection)
- ◆ Enabled (always makes a connection)
- ◆ Active if it sees any character from the serial port
- ◆ Active if it sees a specific (configurable) character from the serial port
- ◆ Modem control signal
- ◆ Modem emulation

To configure Tunnel 1 Connect Mode, perform the following steps.

1. Select **Tunnel 1 > Connect Mode**. Figure 6-10 shows the page that displays.

Figure 6-10 Tunnel Connect Mode Page

Tunnel 1
Tunnel 2

[Statistics](#)
[Accept Mode](#)

[Serial Settings](#)
Connect Mode
[Modem Emulation](#)

[Packing Mode](#)
[Disconnect Mode](#)

Tunnel 1- Connect Mode

Mode:	Disable ▼
Local Port:	<Random>
Host 1:	<None>
Reconnect Timer:	15000 milliseconds
Flush Serial Data:	☐ Enabled ☒ Disabled
Block Serial:	☐ Enabled ☒ Disabled
Block Network:	☐ Enabled ☒ Disabled
Email on Connect:	<None> ▼
Email on Disconnect:	<None> ▼
CP Output:	Group:

Copyright © Lantronix, Inc. 2007-2010. All rights reserved.

2. Enter or modify the fields in Table 6-7.

Table 6-7 Tunnel Connect Mode Fields

Field	Description
Mode	Select the method to be used to attempt a connection to a remote host or device. Choices are: ◆ Always—A connection is attempted until one is made. If the connection gets disconnected, the MatchPort AR retries until it makes a connection. (default) ◆ Disable—An outgoing connection is never attempted. ◆ Any Character—A connection is attempted when any character is read on the serial line. ◆ Start Character—A connection is attempted when the start character for the selected tunnel is read on the serial line.

Table 6-7 Tunnel Connect Mode Fields (continued)

Field	Description
	◆ Modem Control Asserted—A connection is attempted as long as the Modem Control (DSR) is asserted, until a connection is made. Configure the Modem Control Asserted setting (for DSR or DTR) to start a connection when the signal is asserted. The MatchPort AR will try to make a connection indefinitely. If the connection closes, it will not make another connection unless the signal is asserted again. ◆ Modem Emulation—A connection is attempted when triggered by modem emulation AT commands. Note: For the “any character” or “specific character” modes, the MatchPort AR waits and retries the connection. Once it makes a connection and disconnects, it cannot reconnect until it sees “any character” or the “start character” again (depending on the configured setting).
Local Port	Enter the port for use as the local port. A random port is selected by default. Once you have configured a number, click the Random link in the Current Configuration to switch back to random.
Host	Click <None> in the Host field to configure the Host parameters and enter the following fields: ◆ VIP—Enabling the VIP directs the tunnel to connect to a remote Lantronix Virtual IP identified by the VIP Name. When VIP is enabled, the Host 2 field displays. See 11: VIP for more information. Default is Disabled. Note: The MatchPort AR supports configuration of up to sixteen hosts. ◆ VIP Name—Displays configured VIP name, used only if VIP is enabled.Port—Displays configured Port. ◆ Protocol—Select the protocol type (SSH, SSL, TCP, TCP AES, Telnet, UDP, and UDP AES) for use with Connect Mode. The default protocol is TCP. The following are enabled for SSH, TCP, TCP AES, and UDP AES: - SSH Username—Displays configured username, used only if SSH protocol is selected. This is required. The MatchPort AR is the client and the SSH client username must be configured on the remote SSH server before using the MatchPort AR. - TCP Keep Alive—Sends probes to the other end of the connection to ensure that the connection is still valid. Default is 45000 milliseconds. - AES Encrypt/Decrypt Key—Displays presence of key, used only if protocol with AES is selected. When setting AES encryption, both the encrypt key and the decrypt key must be specified. The encrypt key is used for data sent out. The decrypt key is used for receiving data. Both of the keys may be set to the same value. Note: For UDP, the MatchPort AR accepts packets from any device on the network. It send packets to the last device that sent it packets.

Table 6-7 Tunnel Connect Mode Fields (continued)

Field	Description
Reconnect Timer	Enter the reconnect time in milliseconds. The MatchPort AR attempts to reconnect after the specified amount of time when a connection fails or when exiting an established connection. This behavior depends upon the Disconnect Mode. Notes: ◆ When you configure Tunnel - Connect Mode, you can specify a number of milliseconds to attempt to reconnect after a dropped connection has occurred. The default is 1500 milliseconds. ◆ The Reconnect Timer only applies if a Disconnect Mode is configured. With a Disconnect Mode set, the device server maintains a connection until the disconnect mode condition is met (at which time the device server closes the connection). If the tunnel is dropped due to conditions beyond the device server, the device server attempts to re-establish a failed connection when the specified reconnect interval reaches its limit. ◆ Any network-side disconnect is considered an error and a reconnect is attempted without regard to the Connect Mode settings. Simultaneous Connect Mode connections require some Disconnect Mode configurations or the connections will never terminate. See Disconnect Mode on page 54 for more information about the parameters. ◆ If Disconnect Mode is disabled and the network connection is dropped, then the re-establishment of a tunnel connection is governed by the configured Connect Mode settings.
Flush Serial Data	Select whether to flush the serial line when a connection is made. Choices are: ◆ Enabled—Flush the serial line when a connection is made. ◆ Disabled—Do not flush the serial line. This is the default.
Block Serial Data	Select On to block (not tunnel) serial data transmitted to the MatchPort AR.
Block Network Data	Select On to block (not tunnel) network data transmitted to the MatchPort AR.
Email on Connect	Select whether the MatchPort AR sends an email when a connection is made. Select None if you do not want to send an email. Otherwise, select the Email profile to use.
Email on Disconnect	Select whether the MatchPort AR sends an email when a connection is closed. Select None if you do not want to send an email. Otherwise, select the Email profile to use.
CP Output	Enter a CP Group whose value should change when a connection is established and when it is dropped. ◆ Connection value—Specifies the value to set the CP Group to when a connection is established. ◆ Disconnection value—Specifies the value to set the CP Group to when the connection is closed.

3. Click **Submit**.

Multiple Hosts

When you configure two or more hosts in the **Tunnel** web page, **Host Mode** displays. [Figure 6-11](#) shows the page that displays.

Figure 6-11 Host Mode

Tunnel 1		Tunnel 2
Statistics	Serial Settings	Packing Mode
Accept Mode	Connect Mode	Disconnect Mode
Modem Emulation		

Tunnel 1- Connect Mode

Mode:	Disable
Local Port:	<Random>
Host 1	VIP: ☐ Enabled ☒ Disabled
	Address:
	Port: <None>
	Protocol: TCP
	TCP Keep Alive: 45000 milliseconds
Reconnect Timer:	15000 milliseconds
Flush Serial Data:	☐ Enabled ☒ Disabled
Block Serial:	☐ Enabled ☒ Disabled
Block Network:	☐ Enabled ☒ Disabled
Email on Connect:	<None>
Email on Disconnect:	<None>
CP Output:	Group:

Host Mode controls how multiple hosts operate in Connect Mode. The following options are available:

- ◆ Sequential—A Tunnel to the first host is attempted. If the connection fails, the next host specified is attempted. This will continue until a connection is made. If a connection is dropped after a successful connection has been established, tunnel connection attempts begin again from the first host. This is the default.
- ◆ Simultaneous—Tunnel connects to all of the hosts that accept a connection.

To configure Host 2 and other hosts up to a maximum of 16, perform the following steps.

1. Click **<None>** in the Host 2 field. [Figure 6-12](#) shows the page that displays.

Figure 6-12 Host 2 Configuration Fields

Tunnel 1 Tunnel 2	
Statistics	Serial Settings
Accept Mode	Connect Mode Disconnect Mode
Modem Emulation	

Tunnel 1- Connect Mode

Mode:	Disable ▾										
Local Port:	<Random>										
Host 1:	VIP ful2:83, TCP, 45000 msec										
Host 2 ⬆	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 20%;">VIP:</td> <td> ☒ Enabled ☐ Disabled </td> </tr> <tr> <td>VIP Name:</td> <td> 22 </td> </tr> <tr> <td>Port:</td> <td> <None> </td> </tr> <tr> <td>Protocol:</td> <td> TCP ▾ </td> </tr> <tr> <td>TCP Keep Alive:</td> <td> 45000 milliseconds </td> </tr> </table>	VIP:	☒ Enabled ☐ Disabled	VIP Name:	22	Port:	<None>	Protocol:	TCP ▾	TCP Keep Alive:	45000 milliseconds
	VIP:	☒ Enabled ☐ Disabled									
	VIP Name:	22									
	Port:	<None>									
	Protocol:	TCP ▾									
TCP Keep Alive:	45000 milliseconds										
Host 3:	<None>										
Host Mode:	☒ Sequential ☐ Simultaneous										
Reconnect Timer:	15000 milliseconds										
Flush Serial Data:	☐ Enabled ☒ Disabled										
Block Serial:	☐ Enabled ☒ Disabled										
Block Network:	☐ Enabled ☒ Disabled										
Email on Connect:	<None> ▾										
Email on Disconnect:	<None> ▾										
CP Output:	Group:										

Submit

Copyright © Lantronix, Inc. 2007-2010. All rights reserved.

2. Enable **VIP** by clicking **Enabled**. The default is disabled.
3. Enter a **VIP Name**.

Note: See [11: VIP](#) for more information about specifying VIP names.

4. Enter the **Port** number.
5. Select the **Protocol** from the pull-down menu. Depending upon the specified protocol, other options are as follows:
 - ◆ For TCP and Telnet, input the keep alive milliseconds.
 - ◆ For SSH, input the SSH username.
 - ◆ For TCP AES and UDP AES, input the Encrypt/Decrypt keys.

Note: SSL and UDP do not have other options.
6. Repeat the steps until all of your hosts get configured. The maximum is 16.
7. Click **Submit**.

Host List Promotion

The MatchPort AR allows the host list connection order to be specified. There are two types of host modes: Sequential and Simultaneous. Simultaneous connections occur at the same time to all listed hosts.

Sequential host lists establish a prioritized list of tunnels. The host specified as Host 1 will be attempted first. If that fails, it will proceed to Host 2, 3, etc, in the order they are specified. When a connection drops, the cycle starts again with Host 1 and proceeds in order. Establishing the host order is accomplished with host list promotion.

To promote hosts, perform the following steps.

1. Click the arrow icon () of the host you want to promote. [Figure 6-13](#) shows the page that displays.

Figure 6-13 Host List Promotion

Tunnel 1		Tunnel 2	
Statistics	Serial Settings	Packing Mode	
Accept Mode	Connect Mode	Disconnect Mode	
Modem Emulation			

Tunnel 1- Connect Mode

Mode:	Disable
Local Port:	<Random>
Host 1:	VIP ful2:83, TCP, 45000 msec
Host 2 	VIP: ☒ Enabled ☐ Disabled
	VIP Name: 22
	Port: <None>
	Protocol: TCP
	TCP Keep Alive: 45000 milliseconds
Host 3:	<None>
Host Mode:	☒ Sequential ☐ Simultaneous
Reconnect Timer:	15000 milliseconds
Flush Serial Data:	☐ Enabled ☒ Disabled
Block Serial:	☐ Enabled ☒ Disabled
Block Network:	☐ Enabled ☒ Disabled
Email on Connect:	<None>
Email on Disconnect:	<None>
CP Output:	Group:

Copyright © Lantronix, Inc. 2007-2010. All rights reserved.

2. Click **Submit**. The hosts change sequence.

Disconnect Mode

Disconnect Mode ends Accept Mode and Connect Mode connections. It runs in the background of an active connection to determine when to disconnect. When disconnecting, the MatchPort AR shuts down connections gracefully. The following settings end a connection:

- ◆ Stop character received.
- ◆ Timeout period elapsed and no activity. Both Accept Mode and Connect Mode must be idle for a specified time frame.
- ◆ Modem control inactive setting.

Note: To clear data out of the serial buffers upon a disconnect, enable “Flush Serial Data”.

To configure Disconnect Mode, perform the following steps.

1. Click **Tunnel 1 > Disconnect Mode**. Figure 6-14 shows the page that displays.

Figure 6-14 Tunnel 1 Disconnect Mode Web Page

Tunnel 1 Tunnel 2	
Statistics	Serial Settings
Accept Mode	Connect Mode
	Modem Emulation
Packing Mode	
Disconnect Mode	

Tunnel 1- Disconnect Mode

Stop Character:	<None>
Modem Control:	☐ Enabled ☒ Disabled
Timeout:	0 milliseconds
Flush Serial Data:	☐ Enabled ☒ Disabled

Copyright © Lantronix, Inc. 2007-2010. All rights reserved.

2. Enter or modify the fields in [Table 6-8](#).

Table 6-8 Tunnel Disconnect Mode Fields

Field	Description
Stop Character	Enter the stop character in ASCII, hexadecimal, or decimal notation. Select <None> to disable.
Modem Control	Select Enabled to disconnect when the modem control pin is not asserted on the serial line.
Timeout	Enter a time, in milliseconds, for the MatchPort AR to disconnect on a timeout. The value 0 (zero) disables the idle timeout.
Flush Serial Data	Select Enabled to flush the serial data buffer on a disconnection.

3. Click **Submit**.

Modem Emulation

The MatchPort AR supports Modem Emulation mode for devices that send out modem signals. There are two different modes supported:

- ◆ **Command Mode**—Sends verbal response codes.
- ◆ **Data Mode**—Information transferred in gets transferred out.

It is possible to change the default settings for verbose response codes, echo commands, and quiet mode, by using Command Mode commands. The current settings can be overridden; however on reboot, the settings return to the programmed settings.

Configure the connect string as required. The connect string appends to the communication packet when the modem connects to a remote location. It is possible to append additional text to the connect message.

Command Mode

The Modem Emulation 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. All of these commands behave like a modem. For commands that are valid but not applicable to the MatchPort AR, an “OK” message is sent (but the command is silently ignored).

The MatchPort AR attempts to make a Command Mode connection as per the IP/DNS/port numbers defined in Connect Mode. It is possible to override the remote address, as well as the remote port number.

[Table 6-9](#) lists and describes the available commands.

Table 6-9 Modem Emulation Commands and Descriptions

Command	Description
+++	Switches to Command Mode if entered from serial port during connection.
AT?	Help.
ATDT<Address Info>	Establishes the TCP connection to socket (<ipaddress>:<port>).

Table 6-9 Modem Emulation Commands and Descriptions (continued)

Command	Description
ATDP<Address Info>	See ATDT.
ATD	Like ATDT. Dials default Connect Mode remote address and port.
ATD<Address Info>	Sets up a TCP connection. A value of 0 begins a command line interface session.
ATO	Switches to data mode if connection still exists. Vice versa to '+++'.
ATEn	Switches echo in Command Mode (off - 0, on - 1).
ATH	Disconnects the network session.
ATI	Shows modem information.
ATQn	Quiet mode (0 - enable results code, 1 - disable results code.)
ATVn	Verbose mode (0 - numeric result codes, 1 - text result codes.)
ATXn	Command does nothing and returns OK status.
ATUn	Accept unknown commands. (n value of 0 = off. n value of 1 = on.)
AT&V	Display current and saved settings.
AT&F	Reset settings in NVR to factory defaults.
AT&W	Save active settings to NVR.
ATZ	Restores the current state from the setup settings.
ATS0=n	Accept incoming connection. ◆ N value of 0—Disable ◆ N value of 1—Connect automatically ◆ N value of 2+—Connect with ATA command.
ATA	Answer incoming connection (if ATS0 is 2 or greater).
A/	Repeat last valid command.

For commands that can take address information (ATD, ATDT, ATDP), the destination address can be specified by entering the IP Address, or entering the IP Address and port number. For example, <ipaddress>:<port>. The port number cannot be entered on its own.

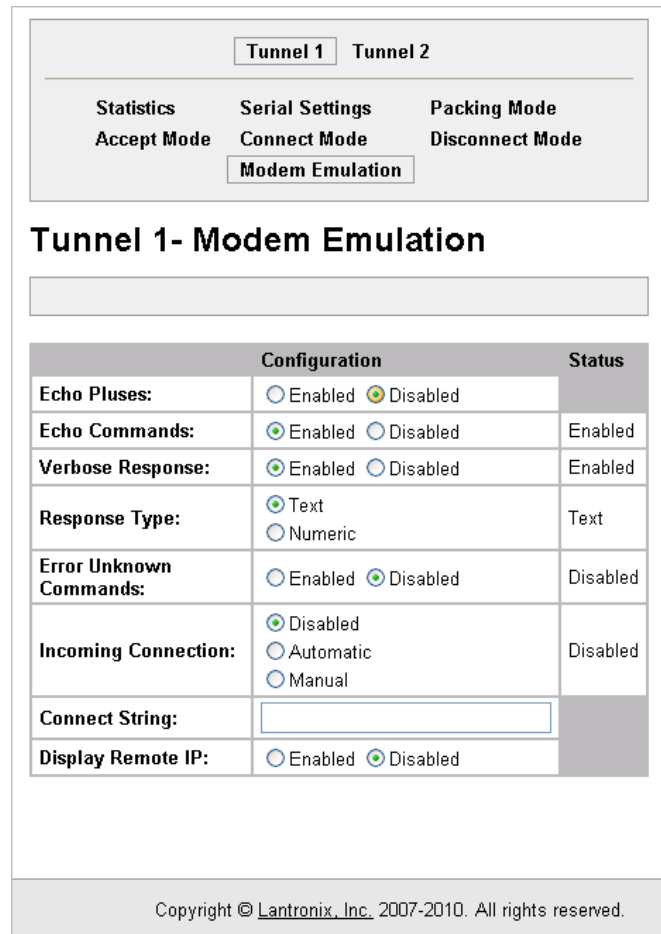
For ATDT and ATDP commands less than 255 characters, the MatchPort AR replaces the last segment of the IP address with the configured Connect Mode remote station address. It is possible to use the last two segments also, if they are under 255 characters. For example, if the address is 100.255.15.5, entering “ATDT 16.6” results in 100.255.16.6.

When using ATDT and ATDP, enter 0.0.0.0 to switch to the Command Line Interface (CLI). Once the CLI is exited by using the CLI exit command, the MatchPort AR reverts to modem emulation mode. By default, the +++ characters are not passed through the connection. Turn on this capability using the **modem echo pluses** command.

To configure modem emulation, perform the following steps.

1. Select **Tunnel 1 > Modem Emulation**. [Figure 6-15](#) shows the page that displays.

Figure 6-15 Tunnel 1 Modem Emulation Web Page



Configuration		Status
Echo Pluses:	☐ Enabled ☒ Disabled	
Echo Commands:	☒ Enabled ☐ Disabled	Enabled
Verbose Response:	☒ Enabled ☐ Disabled	Enabled
Response Type:	☒ Text ☐ Numeric	Text
Error Unknown Commands:	☐ Enabled ☒ Disabled	Disabled
Incoming Connection:	☒ Disabled ☐ Automatic ☐ Manual	Disabled
Connect String:		
Display Remote IP:	☐ Enabled ☒ Disabled	

Copyright © Lantronix, Inc. 2007-2010. All rights reserved.

2. Enter or modify the fields in [Table 6-10](#).

Table 6-10 Tunnel Modem Emulation Fields

Field	Description
Echo Pluses	Select Enable to echo +++ when entering modem Command Mode.
Echo Commands	Select Enable to echo the modem commands to the console.
Verbose Response	Select Enable to send modem response codes out on the serial line.
Response Type	Select the type of response code: Text or Numeric .
Error Unknown Commands	Select whether an ERROR or OK response is sent in reply to unrecognized AT commands. Choices are: ◆ Enabled—ERROR is returned for unrecognized AT commands. ◆ Disabled—OK is returned for unrecognized AT commands. Default is Disabled.

Table 6-10 Tunnel Modem Emulation Fields (continued)

Field	Description
Incoming Connection	Select whether Incoming Connection requests will be disabled, answered automatically, or answered manually. Default is Disabled .
Connect String	Enter the connect string. This modem initialization string prepares the modem for communications. It is a customized string sent with the "CONNECT" modem response code.
Display Remote IP	Selects whether the incoming RING sent on the Serial Line is followed by the IP address of the caller. Default is Disabled .

3. Click **Submit**.

7: Terminal and Host Settings

This chapter describes how to view and configure terminals and hosts. It contains the following sections:

- ◆ Terminal Settings
- ◆ Host Configuration

Terminal Settings

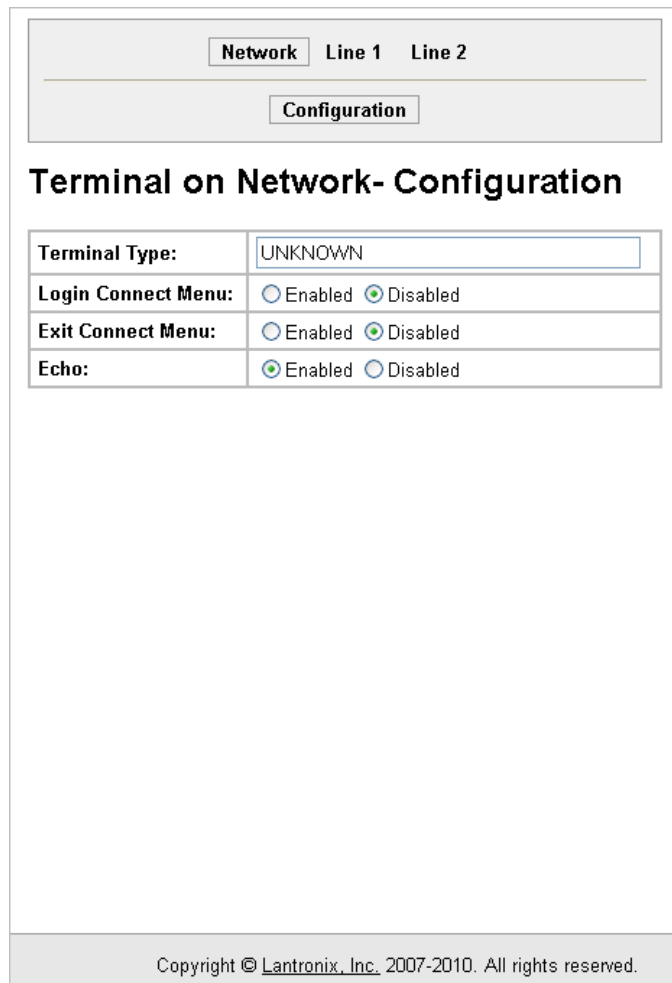
You can configure a terminal on a serial line or on the network by using the Terminal web page. When you click **Terminal** from the Main Menu, Line 1 fields display. To go to the network or line 2, click the Network or Line 2 button.

Network Terminal Configuration

To configure menu features applicable to CLI access via the network, perform the following steps.

1. Click **Terminal > Network**. [Figure 7-1](#) shows the page that displays.

Figure 7-1 Terminal on Network Configuration Web Page



Network Line 1 Line 2	
Configuration	
Terminal on Network- Configuration	
Terminal Type:	UNKNOWN
Login Connect Menu:	☐ Enabled ☒ Disabled
Exit Connect Menu:	☐ Enabled ☒ Disabled
Echo:	☒ Enabled ☐ Disabled

Copyright © Lantronix, Inc. 2007-2010. All rights reserved.

2. Enter or modify the fields in [Table 7-1](#).

Table 7-1 Terminal on Network Configuration Fields

Field	Description
Terminal Type	Enter text to describe the type of terminal. The text will be sent to a host via interpret as command (IAC). Note: IAC is a method to send commands over the network such as send break or start echoing.
Login Connect Menu	Select the interface to display when the user logs in. Choices are: Enabled —Shows the Login Connect Menu. Disabled —Shows the CLI
Exit Connect Menu	Select whether to display a choice for the user to exit the Login Connect Menu and reach the CLI. Choices are: Enabled —Allows the user to exit to the CLI. Disabled —No exit to the CLI.
Echo	Applies only to Connect Mode Telnet connections, not to Accept Mode. Only disable Echo if your terminal echoes, in which case you will see double of each character typed.

3. Click **Submit**.

Line Terminal Configuration

To configure a line to support an attached terminal, perform the following steps.

1. Click **Terminal** on the **Main Menu** and then select the line that is connected to the terminal you want to configure. The default is Line 1. [Figure 7-2](#) shows the page that displays.

Figure 7-2 Terminal on Line 1 Configuration Web Page

Network Line 1 Line 2	
Configuration	
Terminal on Line 1- Configuration	
Terminal Type:	UNKNOWN
Login Connect Menu:	☐ Enabled ☒ Disabled
Exit Connect Menu:	☐ Enabled ☒ Disabled
Send Break:	<None>
Break Duration:	500 milliseconds
Echo:	☒ Enabled ☐ Disabled
Copyright © Lantronix, Inc. 2007-2010. All rights reserved.	

2. Enter or modify the fields in [Table 7-2](#).

Table 7-2 Terminal on Line 1 Configuration Fields

Field	Description
Terminal Type	Enter text to describe the type of terminal. The text will be sent to a host via interpret as command (IAC). Note: IAC is a method to send commands over the network such as send break or start echoing.
Login Connect Menu	Select the interface to display when the user logs in. Choices are: ◆ Enabled —Shows the Login Connect Menu. ◆ Disabled—Shows the CLI
Exit Connect Menu	Select whether to display a choice for the user to exit the Login Connect Menu and reach the CLI. Choices are: ◆ Enabled—A choice allows the user to exit to the CLI. ◆ Disabled—There is no exit to the CLI.

Table 7-2 Terminal on Line 1 Configuration Fields (continued)

Field	Description
Send Break	Enter a Send Break control character, e.g., <control> Y, or blank to disable. When the Send Break control character is received from the network on its way to the serial line, it is not sent to the line; instead, the line output is forced to be inactive (the break condition).
Break Duration	Enter how long the break should last in milliseconds.
Echo	Applies only to Connect Mode Telnet connections, not to Accept Mode. Only disable Echo if your terminal echoes, in which case you will see double of each character typed.

3. Click **Submit**.

Host Configuration

You can configure a remote host by using the Host web page. To configure a remote host, perform the following steps.

1. Click **Host > Host 1** or **Host 2**. [Figure 7-3](#) shows the page that displays.

Figure 7-3 Host Configuration Web Page

The screenshot shows a web interface for host configuration. At the top, there are tabs for 'Host 1' and 'Host 2', with 'Host 1' selected. Below the tabs is a 'Configuration' button. The main heading is 'Host 1- Configuration'. Below this is a form with four fields: 'Name:' with a text input box, 'Protocol:' with radio buttons for 'Telnet' (selected) and 'SSH', 'Remote Address:' with a text input box, and 'Remote Port:' with a text input box containing the value '0'. At the bottom of the page, there is a copyright notice: 'Copyright © Lantronix, Inc. 2007-2010. All rights reserved.'

2. Enter or modify the fields in [Table 7-3](#).

Table 7-3 Host Configuration Fields

Field	Description
Name	Enter a name for the host. This name appears on the Login Connect Menu. To leave a host out of the menu, leave this field blank.
Protocol	Select the protocol to use to connect to the host. Choices are: ◆ Telnet ◆ SSH Note: SSH keys must be loaded or created on the SSH page for the SSH protocol to work.
SSH Username	Appears if you selected SSH as the protocol. Enter a username to select a pre-configured Username/Password/Key (configured on the SSH: Client Users page), or leave it blank to be prompted for a username and password at connect time.
Remote Address	Enter an IP address for the host to which the MatchPort AR will connect.
Remote Port	Enter the port on the host to which the MatchPort AR will connect.

3. Click **Submit**.

8: Configurable Pins Manager

This chapter describes the function and configuration of configurable pins (CPs) by using the Configurable Pins Manager (CPM).

This chapter contains the following sections:

- ◆ [Overview](#)
- ◆ [Configurable Pins](#)
- ◆ [CPM Groups](#)

Overview

Each CP is associated with an external hardware pin. CPs can be configured and used as digital inputs or outputs.

When used as input, device functionality can be triggered based on the state of a CP. For example, an email can be sent when a CP is asserted to a preconfigured level. When used as an output, logic levels of the CP can be manipulated when a preconfigured event occurs on the device server, such as when a tunnel connection is accepted.

CPs are configured and manipulated within a group. Each group is named and is referenced in the feature that is triggering a CP or being triggered by a CP. Sophisticated use of CPs can be accommodated by adding more than one CP into a group.

Default Groups

The MatchPort AR has several predefined CP groups used to assign a CP to a needed function. For instance, when working with an RS485 driver that requires a signal to be asserted when in half-duplex mode, the CP that is driving that signal (chosen by the engineer designing the circuit) is added to the default group named Line1_RS485_HDpx. The MatchPort AR asserts the CP at the correct time via the default group.

Custom Groups

The email, tunneling, and CLI features can interact with CPs. This is accomplished by creating a custom group and adding CPs of your choice into that group. Once a CP group is created and populated with one or more CPs, actions can be triggered when the CPs match a specified value. CPs can be placed in any bit position within a group, allowing for sophisticated use of the available CPs.

Configurable Pins

The CPM web page is used to experimentally configure the state of the CPs. CPs can be changed to be a digital input or a digital output, and whether it is asserted high or low. Changes made on this page do not persist through a reboot.

Rules for configuring a CP are as follows. A CP:

- ◆ Can be in any number of groups.
- ◆ Can be only in one active group. Two groups with the same CP cannot be enabled at the same time.
- ◆ Becomes locked and is not configurable if it is in an enabled group. Disable the group to change the CP configuration.

When you are ready to permanently configure the CPs, see the CPM Groups web page. See [CPM Groups on page 67](#).

Change CPs

To change MatchPort AR CPs, perform the following steps.

1. Click **CPM** on the menu bar and then **CPs** at the top of the page. [Figure 8-1](#) shows the page that displays. [Table 8-1](#) lists and describes the current configuration fields.

Figure 8-1 CPM CPs Page

CPs
Groups

CPM: CPs

Current Configuration

CP	Ref	Configured As	Value	Groups	Active In Group
CP1	P1.13	Input	1	1	Line1_Modem_Ctl_O
CP2	P1.15	Input	1	0	<available>
CP3	P1.17	Input	1	0	<available>
CP4	P1.19	Input	1	0	<available>
CP5	P1.29	Input	0	0	<available>
CP6	P1.31	Input	1	1	<available>
CP7	P1.33	Input	0	1	<available>

CP Status

Name	CP1						
State	Enabled AND Locked						
Type	Input						
Value	1 (0x1)						
Bit	6	5	4	3	2	1	0
Level							+
I/O							I
Logic							
Binary	x	x	x	x	x	x	1
CP#							1
Groups	Line1_Modem_Ctl_O						

Copyright © [Lantronix, Inc.](#) 2007-2010. All rights reserved.

Table 8-1 CPM CPs Current Configuration Fields and Descriptions

Field	Description
CP	Indicates the configurable pin number.
Ref	Indicates the hardware pin number associated with the CP.
Configured As	Shows the current CP configuration. A CP configured as Input is set to read input. A CP configured as Output drives data out of the MatchPort AR.

Table 8-1 CPM CPs Current Configuration Fields and Descriptions (continued)

Field	Description
Value	Shows the current value of the CP.
Groups	Indicates the number of groups in which the CP is a member.
Active In Group	Shows the group in which the CP is active. A CP can be a member of several groups. However, it may only be active in one group.

- Click a CP number (CP column) to display the status of that pin. The status is shown in the CP Status section of the web page. [Table 8-2](#) lists and describes the fields for the selected CP.

Table 8-2 CPM CPs Status Fields and Descriptions

Fields	Description
Name	Shows the CP number.
State	Shows the current enable state of the CP. On the MatchPort AR the CP state is always enabled.
Type	Indicates whether the CP is set for input or output.
Value	Shows the current value of the CP.
Bit	Shows the bit position. CPs are always displayed in bit position zero.
Level	Indicates the voltage level of the CP. A plus sign (+) indicates the CP is asserted (the voltage is high). A minus sign (-) indicates the CP voltage is low.
I/O	Indicates the current status of the pin: ◆ I—Input ◆ O—Output ◆ <blank—Unassigned
Logic	Indicates that the CP is inverted by displaying an "I".
Binary	Shows the assertion value of the corresponding bit.
CP#	Shows the CP number.
Groups	Lists the groups in which the CP is a member.

Note: To modify a CP, all groups in which it is a member must be disabled. The changes to a CP are not saved in FLASH.

CPM Groups

The CPM Groups page allows for the adding, removing, and managing CP groups. A group, based on its state, can trigger outside events such as sending email messages. Only an enabled group can be a trigger.

View CP Group Status

Click the CP group name in the Current Configuration section of the page. [Table 8-3](#) lists and describes the fields in the groups status section of the page.

Table 8-3 CPM Group Status Fields and Descriptions

Field	Description
Name	Shows the CP Group name.
State	Shows the current state of the CP group. Locked groups are Lantronix default groups and cannot be deleted. Use the button in this field to enable or disable the group.
Value	Shows the current CP group value.
Bit	Displays the 7-bit positions for the CPs in the group.
Level	Indicates the voltage level of the CP. A plus sign (+) indicates the CP bit is asserted (the voltage is high). A minus sign (-) indicates the CP voltage is low.
I/O	Indicates the current status of the pin: ◆ I—Input ◆ O—Output ◆ <blank>—Unassigned
Logic	Indicates the output of the CP. An "I" indicates the CP output is inverted. A blank field indicates that the CP is not inverted.
Binary	Shows the assertion value of the corresponding bit. An "x" means that the bit is unassigned in the group.
CP#	Shows the configurable pin number and its bit position in the CP group.

Add Custom CP Groups

To add a custom MatchPort AR CP group, perform the following steps.

1. Click **CPM** on the menu bar and then **Groups** at the top of the page. [Figure 8-2](#) shows the page that displays. [Table 8-4](#) lists and describes the fields in the Current Configuration section of the page.

Figure 8-2 CPM Groups Page

CPs Groups

CPM: Groups

Current Configuration

Group Name	State	CP Info
I2C	Disabled	2 CPs Assigned
Line1_Modem_Ctl_In	Disabled	0 CPs Assigned
Line1_Modem_Ctl_O	Enabled	1 CP Assigned
Line1_RS485_HDpx	Disabled	0 CPs Assigned
Line1_RS485_Select	Disabled	0 CPs Assigned
Line2_Modem_Ctl_In	Disabled	0 CPs Assigned
Line2_Modem_Ctl_O	Disabled	0 CPs Assigned

Create Group:

Group Status

Name	Line1_Modem_Ctl_In						
State	Disabled AND Locked, user may Enable/Disable or Add/Remove CP Enable 						
Value	Disabled						
Bit	6	5	4	3	2	1	0
Level							
I/O							
Logic							
Binary	x	x	x	x	x	x	x
CP#							

CP1
at bit 0
as
☐ Assert Low

Copyright © [Lantronix, Inc.](#) 2007-2010. All rights reserved.

Table 8-4 CPM Groups Current Configuration Fields and Descriptions

Fields	Description
Group Name	Shows the CP group name.
State	Indicates whether the group is enabled or disabled.
CP Info	Shows the number of CPs in the group.

2. Enter a group name in the Create Group text box and click Submit.
3. Add CPs with the Add button. Be sure to specify:
 - ◆ CP # .
 - ◆ Bit position.
 - ◆ Input or output.
 - ◆ Assertion level. Check the Assert Low box to specify inverted assertion.

Remove Custom CP Groups

To remove a customer CP group, perform the following steps.

1. Click on the group name that you want to remove. The name is in the Group Name column.
2. Click the red "x" that appears next to the name in the Group Status table.
3. Click OK to confirm the deletion.

Remove CPs from CP Groups

To remove a CP from a CP group, perform the following steps.

1. Click on the Group in the Group Name column that contains the CP to be removed.
2. Select the CP from the Remove drop-down list at the bottom of the page.
3. Click Remove.

9: Services Settings

This chapter describes the available services and how to configure each. It contains the following sections:

- ◆ [DNS Status and Cache](#)
- ◆ [PPP Configuration](#)
- ◆ [SNMP Configuration](#)
- ◆ [FTP](#)
- ◆ [TFTP](#)
- ◆ [Syslog](#)
- ◆ [HTTP](#)
- ◆ [RSS](#)
- ◆ [LPD](#)

DNS Status and Cache

The primary and secondary domain name system (DNS) addresses come from the active interface. The static addresses displayed on the Network Interface Configuration web page may be overridden by DHCP or BOOTP. The DNS web page enables you to view the status and cache.

When a DNS name is resolved using a forward lookup, the results get stored in the DNS cache temporarily. The MatchPort AR checks the cache when performing forward lookups. Each item in the cache eventually times out and gets removed automatically after a certain period or you can delete it manually.

To view the DNS status and cache, perform the following steps.

1. Click **DNS** on the Main Menu. [Figure 9-1](#) shows the page that displays.

Figure 9-1 DNS Status and Cache Web Page

DNS

Current Status

Primary DNS:	172.19.1.1 (DHCP)
Secondary DNS:	172.19.1.2 (DHCP)

DNS Cache

There are no entries in the cache.

Copyright © Lantronix, Inc. 2007-2010. All rights reserved.

PPP Configuration

The Point-to-Point Protocol (PPP) establishes a direct connection between two nodes. It defines a method for data link connectivity between devices using physical layers (such as serial lines). The MatchPort AR supports two types of PPP authentication: Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP). Both of these authentication methods require the configuration of a username and password.

PAP authentication offers a straightforward method for the peer to determine its identity. Upon the link establishment, the user ID and password are repeatedly sent to the authenticator until it is acknowledged or the connection is terminated. However, PAP is not a strong authentication process. There is no protection against trial-and-error attacks. The peer is responsible for the frequency of the authentication communication attempts.

CHAP is a more secure method than PAP. It works by sending a challenge message to the connection requestor. Using a one-way hash function, the requestor responds with its value. If the value matches the server's own calculations, authentication is provided. Otherwise, the connection is terminated.

Note: RFC1334 defines both CHAP and PAP.

The MatchPort AR also supports authentication scheme of “None” when no authentication is required during link negotiation.

Since the MatchPort AR does not support Network Address and Port Translation (NAPT), static routing table entries must be added to the serial-side and network-side devices (both of which are external devices).

Use the MatchPort AR Web Manager or CLI to configure a network link using PPP over a serial line. Turn off Connect Mode, Accept Mode, and Command mode before enabling PPP. The MatchPort AR acts as the server side of the PPP link; it can require authentication and assign an IP address to the peer. Upon PPP configuration, IP packets are routed between Ethernet and PPP interfaces.

The MatchPort AR does not perform network address translation (NAT) between the serial-side network interface and the Ethernet/WLAN network interface. Therefore, to pass packets through the MatchPort AR, a static route must be configured on both the PPP Peer device and the remote device it wishes to communicate with. The static route in the PPP Peer device must use the PPP Local IP Address as its gateway, and the static route in the remote device must use the Ethernet/WLAN IP Address of the MatchPort AR as its gateway.

To configure PPP, perform the following steps.

1. Click **PPP** on the Main Menu. [Figure 9-2](#) shows the page that displays.

Figure 9-2 PPP Configuration Web Page

Line 1
Line 2

Configuration

PPP on Line 1- Configuration

WARNING: Serial protocol is not PPP.

Local IP Address:	192.168.99.1/24
Peer IP Address:	192.168.99.2
Authentication Mode:	☐ None ☒ PAP ☐ CHAP ☐ MS-CHAP ☐ MS-CHAPV2
Username:	test
Password:	<Configured>

Copyright © Lantronix, Inc. 2007-2010. All rights reserved.

2. Enter or modify the fields in [Table 9-1](#).

Table 9-1 PPP Configuration Fields

Field	Description
Local IP Address	Enter the IP address assigned to the MatchPort AR's PPP interface.
Peer IP Address	Enter the IP address assigned to the peer (when requested during negotiation).
Authentication Mode	Choose the authentication mode: ◆ None—No authentication is required. ◆ PAP—Password Authentication Protocol. ◆ CHAP—Challenge–Handshake Authentication Protocol. ◆ MS-CHAP—Microsoft Challenge–Handshake Authentication Protocol. ◆ MS-CHAPV2—Microsoft Challenge–Handshake Authentication Protocol Version 2.
Username	Enter a username if authentication will be used on the PPP interface. The peer must be configured to use the same username.
Password	Enter a password if authentication will be used on the PPP interface. The peer must be configured to use the same password.

3. Click **Submit**.

SNMP Configuration

Simple Network Management Protocol (SNMP) is a network management tool that monitors network devices for conditions that need attention. The Web Manager configured SNMP service sends traps whenever a request for information that contains an incorrect community name and does not match an accepted system name for the service gets sent.

To configure SNMP, perform the following steps.

1. Click **SNMP** on the Main Menu. [Figure 9-3](#) shows the page that displays.

Figure 9-3 SNMP Web Page

SNMP

SNMP Agent: ☐ On ☐ Off

Read Community:

Write Community:

System Contact:

System Name:

System Description:

System Location:

Enable Traps: ☐ On ☐ Off

Primary Trap Dest IP:

Secondary Trap Dest IP:

Current Configuration

SNMP Agent Status:	Running (On)
Read Community:	<Configured> [Delete]
Write Community:	<Configured> [Delete]
System Contact:	<None>
System Name:	EDS2100 [Delete]
System Description:	<Default>
System Location:	<None>
Traps Enabled:	On
Primary Trap Dest IP:	<None>
Secondary Trap Dest IP:	<None>

Copyright © Lantronix, Inc. 2007-2010. All rights reserved.

2. Enter or modify the fields in [Table 9-2](#).

Table 9-2 SNMP Fields

Field	Description
SNMP Agent	Select On to enable SNMP.
Read Community	Enter the SNMP read-only community string.
Write Community	Enter the SNMP read/write community string.
System Contact	Enter the name of the system contact.

Table 9-2 SNMP Fields (continued)

Field	Description
System Name	Enter the system name.
System Description	Enter the system description.
System Location	Enter the system location.
Traps Enabled	Select On to enable the transmission of the SNMP cold start trap messages. This trap is generated during system boot.
Primary Trap Dest IP	Enter the primary SNMP trap host.
Secondary Trap Dest IP	Enter the secondary SNMP trap host.

3. Click **Submit**.

Note: You can delete the read and write communities, and system name by clicking the **[Delete]** link in the **Current Configuration** table.

FTP

The FTP web page shows the FTP configuration and statistics about the FTP server. To configure FTP, perform the following steps.

1. Click **FTP** on the Main Menu. [Figure 9-4](#) shows the page that displays.

Figure 9-4 FTP Web Page

FTP

Configuration	
State:	☒ Enabled ☐ Disabled
Admin Username:	admin
Admin Password:	<Configured>

Statistics	
Status:	Running
Connections Rejected:	0
Connections Accepted:	6
Active Connections:	0
Last Client:	172.19.212.2:26677

Copyright © Lantronix, Inc. 2007-2010. All rights reserved.

2. Enter or modify the fields in [Table 9-3](#).

Table 9-3 FTP Fields

Field	Description
State	Select Enabled to enable the FTP server.
Admin Username	Enter the username to use when logging in via FTP.
Admin Password	Enter the password to use when logging in via FTP.

TFTP

In the TFTP web page, you can configure the server, and view the status and statistics. To configure TFTP server, perform the following steps.

1. Click **TFTP** on the Main Menu. [Figure 9-5](#) shows the page that displays.

Figure 9-5 TFTP Server Web Page

TFTP Server

Configuration	
State:	☒ Enabled ☐ Disabled
Allow File Creation:	☐ Enabled ☒ Disabled
Allow Firmware Update:	☐ Enabled ☒ Disabled
Allow XCR Import:	☐ Enabled ☒ Disabled

Statistics	
Status:	Running
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

Copyright © Lantronix, Inc. 2007-2010. All rights reserved.

2. Enter or modify the fields in [Table 9-4](#).

Table 9-4 TFTP Server Fields

Field	Description
State	Select Enabled to enable the TFTP server.
Allow File Creation	Select whether to allow the creation of new files stored on the TFTP server.
Allow Firmware Update	Specifies whether or not the TFTP Server is allowed to accept a firmware update for the device. An attempt to update firmware is recognized based on the name of the file. Note: TFTP cannot authenticate the client so the device is open to malicious updates.

Table 9-4 TFTP Server Fields (continued)

Field	Description
Allow XCR Import	Specifies whether or not the TFTP server is allowed to accept an XML configuration file for update. An attempt to import the configuration is recognized based on the name of the file. Note: TFTP cannot authenticate the client so the device is open to malicious updates.

Syslog

In the Syslog web page, you can configure settings, and view statistics and status. To configure the Syslog, perform the following steps.

Note: The Syslog file gets saved to IRAM and gets discarded when the MatchPort AR reboots. Saving the Syslog file to a server that supports remote logging services (see RFC 3164) allows the administrator to save the complete Syslog history. The default port is 514.

1. Click **Syslog** on the Main Menu. [Figure 9-6](#) shows the page that displays.

Figure 9-6 Syslog Web Page

Syslog

Configuration	
State:	☐ Enabled ☒ Disabled
Host:	
Local Port:	514
Remote Port:	514
Severity Log Level:	None v

Statistics	
Status:	Inactive
Messages Sent:	0
Messages Failed:	0

Copyright © Lantronix, Inc. 2007-2010. All rights reserved.

2. Enter or modify the fields in [Table 9-5](#)

Table 9-5 Syslog Fields

Field	Description
State	Select to enable or disable the syslog.
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 MatchPort AR from which system logs are sent.
Remote Port	Enter the number of the port on the remote server that supports logging services. The default is 514 .
Severity Log Level	From the drop-down box, select the minimum level of system message the MatchPort AR 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

HyperText Transfer Protocol (HTTP) is an application layer standard for Internet documents. HTTP defines how messages get formatted and transmitted. It also defines the actions web servers and browsers should take in response to different commands. HTTP Authentication enables the requirement of usernames and passwords for access to the MatchPort AR device.

The HTTP web page contains the following sub-menus:

- ◆ Statistics—Viewing statistics such as bytes received and transmitted, bad requests, authorizations required, etc.
- ◆ Configuration—Configuring and viewing the current configuration.
- ◆ Authentication—Configuring and viewing the authentication.

HTTP Statistics

To view HTTP statistics, perform the following steps.

1. Click **HTTP > Statistics**. Statistics is the default. [Figure 9-7](#) shows the page that displays.

Figure 9-7 HTTP Statistics Web Page

Statistics Configuration Authentication	
HTTP Statistics	
Rx Bytes	257405
Tx Bytes	2513036
200 - OK	341
400 - Bad Request	13
401 - Authorization Required	49
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:	50 entries (8046 bytes) [View] [Clear]
Copyright © Lantronix, Inc. 2007-2010. All rights reserved.	

Note: The HTTP log is a scrolling log, with the last Max Log Entries cached and viewable. You can change the maximum number of entries that can be viewed on the HTTP Configuration Web Page.

HTTP Configuration

To configure HTTP, perform the following steps.

1. Click **HTTP > Configuration**. [Figure 9-8](#) shows the page that displays.

Figure 9-8 HTTP Configuration Web Page

Statistics
Configuration
Authentication

HTTP Configuration

HTTP Server: ☒ On ☐ Off

HTTP Port:

HTTPS Port:

HTTPS Protocols

SSL3: ☐ Enable ☐ Disable

TLS1.0: ☐ Enable ☐ Disable

TLS1.1: ☐ Enable ☐ Disable

Max Timeout: seconds

Max Bytes:

Logging: ☐ On ☐ Off

Max Log Entries:

Log Format:

Current Configuration

HTTP Status:	On (running)
HTTP Port:	80
HTTPS Port:	443
HTTPS Protocols:	SSL3, TLS1.0, TLS1.1
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"
Logs:	50 entries (8022 bytes) View Clear

Copyright © Lantronix, Inc. 2007-2010. All rights reserved.

2. Enter or modify the fields in [Table 9-6](#).

Table 9-6 HTTP Configuration Fields

Field	Description
HTTP Server	Select On to enable the HTTP server.
HTTP Port	Enter the port for the HTTP server to use. The default is 80 .
HTTPS Port	Enter the port for the HTTPS server to use. The default is 443 . The HTTP server only listens on the HTTPS Port when an SSL certificate is configured.
HTTPS Protocols	Select to enable or disable the following protocols: ◆ SSL3—Secure Sockets Layer version 3 ◆ TLS1.0—Transport Layer Security version 1.0. TLS 1.0 is the successor of SSL3 as defined by the IETF. ◆ TLS1.1—Transport Layer Security version 1.1 The protocols are enabled by default. Note: A server certificate and associated private key needs to be installed in the SSL configuration section to use HTTPS.
Max Timeout	Enter the maximum time for the HTTP server to wait when receiving a request. This prevents Denial-of-Service (DoS) attacks. The default is 10 seconds.
Max Bytes	Enter the maximum number of bytes the HTTP server accepts when receiving a request. The default is 40 kB (this prevents DoS attacks).
Logging	Select On to enable HTTP server logging.
Max Log Entries	Sets the maximum number of HTTP server log entries. Only the last Max Log Entries are cached and viewable.
Log Format	Set the log format string for the HTTP server. Follow these Log Format rules: ◆ %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}i—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 '-') ◆ %t—Timestamp HH:MM:SS (same as Apache '%(%H:%M:%S)t' or '%(%T)t') ◆ %u—Remote user (could be bogus for 401 status) ◆ %U—URL path info ◆ %r—Rirst line of request (same as '%m %U%q <version>') ◆ %s—Return status

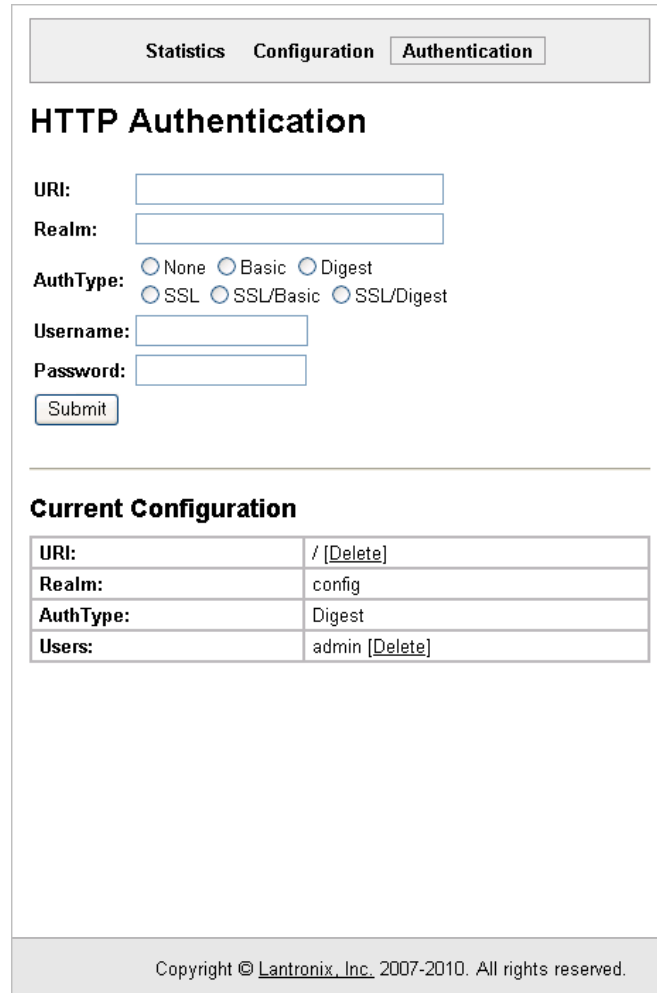
3. Click **Submit**.

HTTP Authentication

To configure HTTP authentication, perform the following steps.

1. Click **HTTP > Authentication**. [Figure 9-9](#) shows the page that displays.

Figure 9-9 HTTP Authentication Web Page



Statistics Configuration **Authentication**

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]

Copyright © Lantronix, Inc. 2007-2010. All rights reserved.

2. Enter or modify the fields in [Table 9-7](#).

Table 9-7 HTTP Authentication Fields

Fields	Description
URI	Enter the Uniform Resource Identifier (URI). Note: The URI must begin with '/' to refer to the filesystem.
Realm	Enter the domain, or realm, used for HTTP. Required with the URI field.

Table 9-7 HTTP Authentication Fields (continued)

Fields	Description
Auth Type	Select the authentication type: ◆ None—No authentication is necessary. ◆ Basic—Encodes passwords using Base64. ◆ Digest—Encodes passwords using MD5. ◆ SSL—The page can only be accessed over SSL (no password is required). ◆ SSL/Basic—The page is accessible only over SSL and encodes passwords using Base64. ◆ SSL/Digest—The page is accessible only over SSL and encodes passwords using MD5.
Username	Enter the Username used to access the URI. <i>Note:</i> More than one username per URI is permitted. Click Submit and enter the next Username.
Password	Enter the Password for the Username.

3. Click **Submit**.

Notes:

- ◆ You can delete URI and users by clicking the **[Delete]** link in the **Current Configuration** table.
- ◆ The URI, realm, username, and password are user-specified, free-form fields. The URI must match the directory created on the filesystem.

RSS

Really Simple Syndication (RSS) (sometimes referred to as Rich Site Summary) is a method of sending online content to Web users. Instead of actively searching for MatchPort AR configuration changes, RSS enables viewing relevant and new information regarding changes made to the MatchPort AR via an RSS publisher. RSS can be stored to the file system `cfg_log.txt` file.

To configure RSS, perform the following steps.

1. Click **RSS** on the Main Menu. [Figure 9-10](#) shows the page that displays.

Figure 9-10 RSS Web Page

RSS

RSS Feed:	☐ On ☒ Off
Persistent:	☐ On ☒ Off
Max Entries:	100

Current Status

Data:	0 entries (0 bytes) [View] [Clear]
-------	--

Copyright © Lantronix, Inc. 2007-2010. All rights reserved.

2. Enter or modify the fields in [Table 9-8](#).

Table 9-8 RSS Fields

Fields	Description
RSS Feed	Select On to enable RSS feeds to an RSS publisher.
Persistent	Select On to enable the RSS feed to be written to a file (cfg_log.txt) and to be available across reboots.
Max Entries	Sets the maximum number of log entries. Only the last Max Entries are cached and viewable.

Note: You can view and clear settings in the **Current Status** table by clicking [\[View\]](#) or [\[Clear\]](#).

LPD

The MatchPort AR acts as a print server if a printer gets connected to one of its serial ports. Clicking the Line Printer Daemon (LPD) link in the Main Menu displays the LPD web page. The LPD web page has three sub-menus for viewing print queue statistics, changing print queue configuration, and printing a test page. Because the LPD lines operate independently, you can specify different configuration settings for each.

LPD Statistics

To view LPD statistics, perform the following steps.

1. Click **LPD** on the Main Menu. [Figure 9-11](#) shows the page that displays.

Figure 9-11 LPD Web Page

The screenshot shows the LPD web interface. At the top, there are two tabs: 'LPD 1' and 'LPD 2'. Below the tabs is a navigation bar with three buttons: 'Statistics' (which is highlighted), 'Configuration', and 'Print Test Page'. The main content area is titled 'LPD 1- Statistics' and contains a table with the following data:

Jobs Printed:	0
Bytes Printed:	0
Current Client:	No device is connected.
Last Client:	No device has connected.

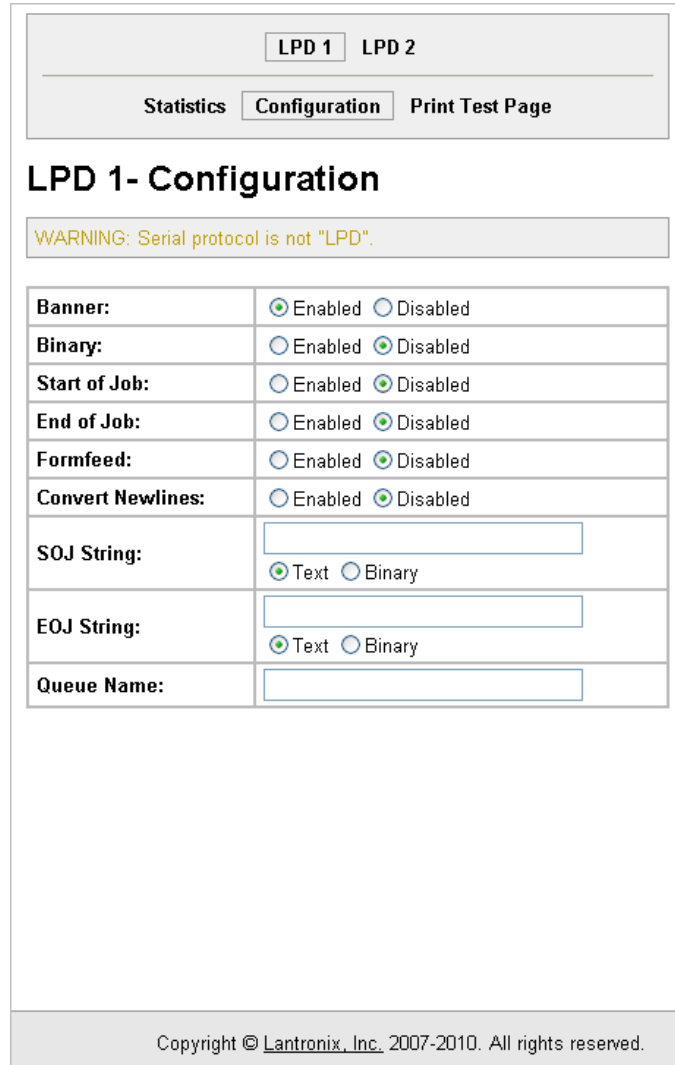
At the bottom of the page, there is a copyright notice: 'Copyright © Lantronix, Inc. 2007-2010. All rights reserved.'

LPD Configuration

To configure LPD, perform the following steps.

1. Click **LPD > Configuration**. [Figure 9-12](#) shows the page that displays.

Figure 9-12 LPD Configuration Web Page



LPD 1 LPD 2

Statistics Configuration Print Test Page

LPD 1- Configuration

WARNING: Serial protocol is not "LPD".

Banner:	☒ Enabled ☐ Disabled
Binary:	☐ Enabled ☒ Disabled
Start of Job:	☐ Enabled ☒ Disabled
End of Job:	☐ Enabled ☒ Disabled
Formfeed:	☐ Enabled ☒ Disabled
Convert Newlines:	☐ Enabled ☒ Disabled
SOJ String:	 ☒ Text ☐ Binary
EOJ String:	 ☒ Text ☐ Binary
Queue Name:	

Copyright © Lantronix, Inc. 2007-2010. All rights reserved.

2. Enter or modify the fields in [Table 9-9](#).

Table 9-9 LPD Configuration Fields

Field	Description
Banner	Select Enabled to print the banner even if the print job does not specify to do so. Selected by default.
Binary	Select Enabled for the MatchPort AR to pass the entire file to the printer unchanged. Otherwise, the MatchPort AR passes only valid ASCII and valid control characters to the printer. Valid control characters include the tab, linefeed, formfeed, backspace, and newline characters. All others are stripped. Disabled by default.

Table 9-9 LPD Configuration Fields (continued)

Field	Description
Start of Job	Select Enabled to print a "start of job" string before sending the print data.
End of Job	Select Enabled to send an "end of job" string.
Formfeed	Select Enabled to force the printer to advance to the next page at the end of each print job.
Convert Newlines	Select Enabled to convert single newlines and carriage returns to DOS-style line endings.
SOJ String	If Start of Job (above) is enabled, enter the string to be sent to the printer at the beginning of a print job. The limit is 100 characters. Indicate whether the string is in text or binary format.
EOJ String	If End of Job (above) is enabled, enter the string to send at the end of a print job. The limit is 100 characters. Indicate whether the string is in text or binary format.
Queue Name	To change the name of the print queue, enter a new name. The name cannot have white space in it and is limited to 31 characters. The default is LPDQueueX (for line number X)

10: Security Settings

The MatchPort AR supports Secure Shell (SSH) and Secure Sockets Layer (SSL). SSH is a network protocol for securely accessing a remote device. SSH provides a secure, encrypted communication channel between two hosts over a network. It provides authentication and message integrity services.

Secure Sockets Layer (SSL) is a protocol that manages data transmission security over the Internet. It uses digital certificates for authentication and cryptography against eavesdropping and tampering. It provides encryption and message integrity services. SSL is widely used for secure communication to a web server. SSL uses certificates and private keys.

Note: The MatchPort AR supports SSLv3 and its successors, TLS1.0 and TLS1.1. An incoming SSLv2 connection attempt is answered with an SSLv3 response. If the initiator also supports SSLv3, SSLv3 handles the rest of the connection.

This chapter contains the following sections:

- ◆ SSH Server Host Keys
- ◆ SSH Server Authorized Users
- ◆ SSH Client Known Hosts
- ◆ SSH Client Users
- ◆ SSL Certificates
- ◆ SSL RSA or DSA
- ◆ SSL Certificates and Private Keys
- ◆ SSL Utilities
- ◆ SSL Configuration

SSH Server Host Keys

The SSH Server Host Keys web page opens when you click SSH from the Main Menu. It has four sub-menus for viewing and changing SSH server host keys, SSH server authorized keys, SSH client known hosts, and SSH client users.

Note: SSH keys may be created on another computer and uploaded to the MatchPort AR. For example, use the **ssh-keygen -b 1024 -t dsa** command to create a 1024-bit DSA key pair. SSH Keys from other programs may be converted to the required MatchPort AR format. Use **Open SSH** to perform the conversion.

To create or upload SSH server host keys, perform the following steps.

1. Click **SSH** on the Main Menu. [Figure 10-1](#) shows the page that displays.

Figure 10-1 SSH Server Host Keys Web Page

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:	No RSA Key Configured
Public DSA Key:	No DSA Key Configured

Copyright © Lantronix, Inc. 2007-2010. All rights reserved.

2. Enter or modify the fields in [Table 10-1](#).

Table 10-1 SSH Server Host Keys Fields

Field	Description
Upload Keys	
Private Key	Enter the path and name of the existing private key you want to upload or use the Browse 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 Browse button to select the key.
Key Type	Select a key type to use. ◆ RSA—Use this key with SSH1 and SSH2 protocols. ◆ DSA—Use this key with the SSH2 protocol.

Table 10-1 SSH Server Host Keys Fields (continued)

Field	Description
Create New Keys	
Key Type	Select a key type to use. ◆ RSA—Use this key with SSH1 and SSH2 protocols. ◆ DSA—Use this key with the SSH2 protocol.
Bit Size	Select a bit length for the new key: 512, 768, 1024. Using a larger bit size takes more time to generate the key. Approximate times are: ◆ 10 seconds for a 512 bit RSA Key ◆ 15 seconds for a 768 bit RSA Key ◆ 1 minute for a 1024 bit RSA key ◆ 30 seconds for a 512 bit DSA key ◆ 1 minute for a 768 bit DSA key ◆ 2 minutes for a 1024 bit DSA key Note: Some SSH clients require RSA host keys to be at least 1024 bits long. Note: MatchPort AR generates keys up to 1024 bits long. It can work with larger keys (up to 2048 bit) if they are imported or otherwise created.

3. Click **Submit**.

SSH Server Authorized Users

You can change SSH server settings for Authorized Users which are accounts that enable access to the MatchPort AR. For example, these SSH accounts can be used to log into the CLI or open an SSH connection to a device port. Every account must have a password.

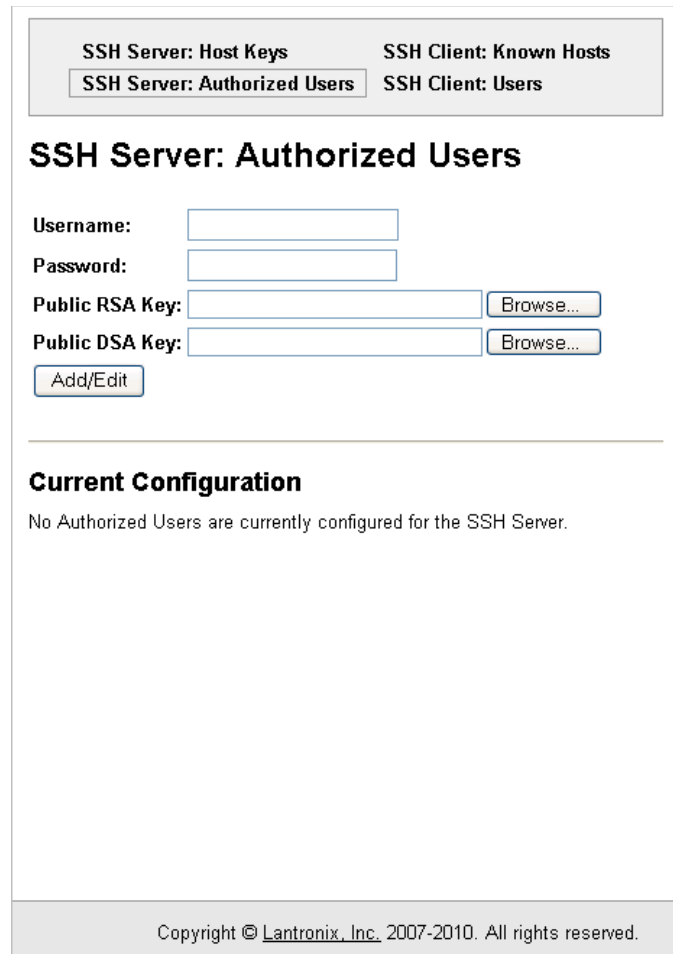
The public keys are optional and only necessary if public key authentication is required. Using public key authentication allows a connection to be made without a password.

Under Current Configuration, User has a Delete User link, and Public RSA Key and Public DSA Key have View Key and Delete Keylinks. 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.

To configure the SSH server for authorized users, perform the following steps.

1. Click **SSH > Server Authorized Users**. [Figure 10-2](#) shows the page that displays.

Figure 10-2 SSH Server Authorized Users Web Page



2. Enter or modify the fields in [Table 10-2](#).

Table 10-2 SSH Server Authorized Users Fields

Field	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 Browse 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 Browse button to select the key. If authentication is successful with the key, no password is required.

3. Click **Submit**.

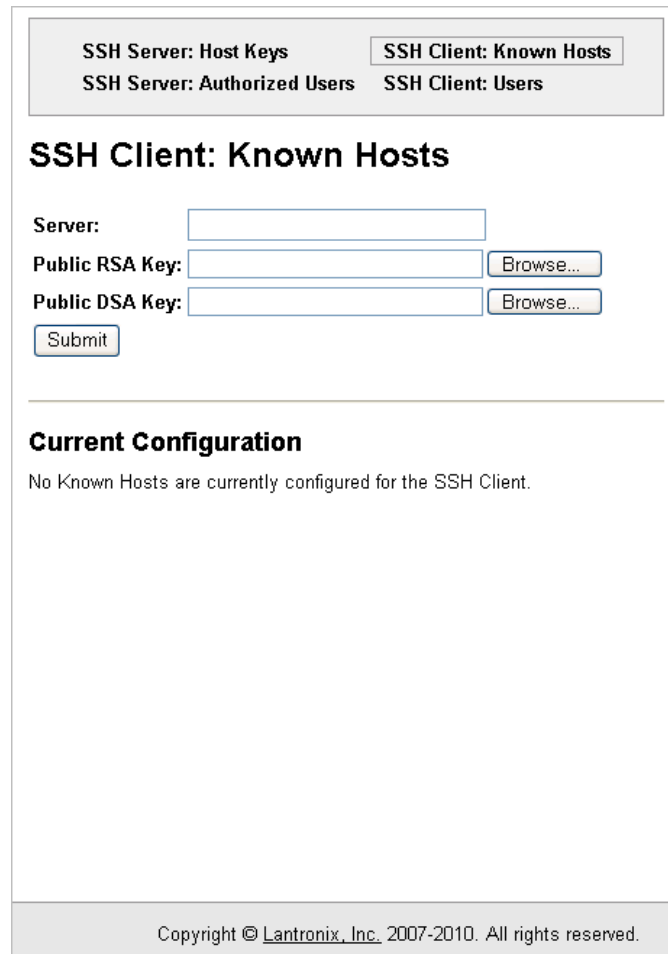
SSH Client Known Hosts

You can change SSH client settings for known hosts. You do not have to complete the fields on this page for communication to occur. However, adding information in the fields adds another layer of security that protects against Man-In-The-Middle (MITM) attacks.

To configure the SSH client for known hosts, perform the following steps.

1. Click **SSH > Client Known Hosts**. [Figure 10-3](#) shows the page that displays.

Figure 10-3 SSH Client Known Hosts Web Page



2. Enter or modify the fields in [Table 10-3](#).

Table 10-3 SSH Client Known Hosts Fields

Field	Description
Server	Enter the name or IP address of a known host. If you enter a server name, the name should match the name of the server used as the Remote Address 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 Browse button to select the key.

Table 10-3 SSH Client Known Hosts Fields (continued)

Field	Description
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 Browse button to select the key.

3. Click **Submit**.

Note: You can delete stored settings when the **[Delete]** link displays in the **Current Configuration** table.

SSH Client Users

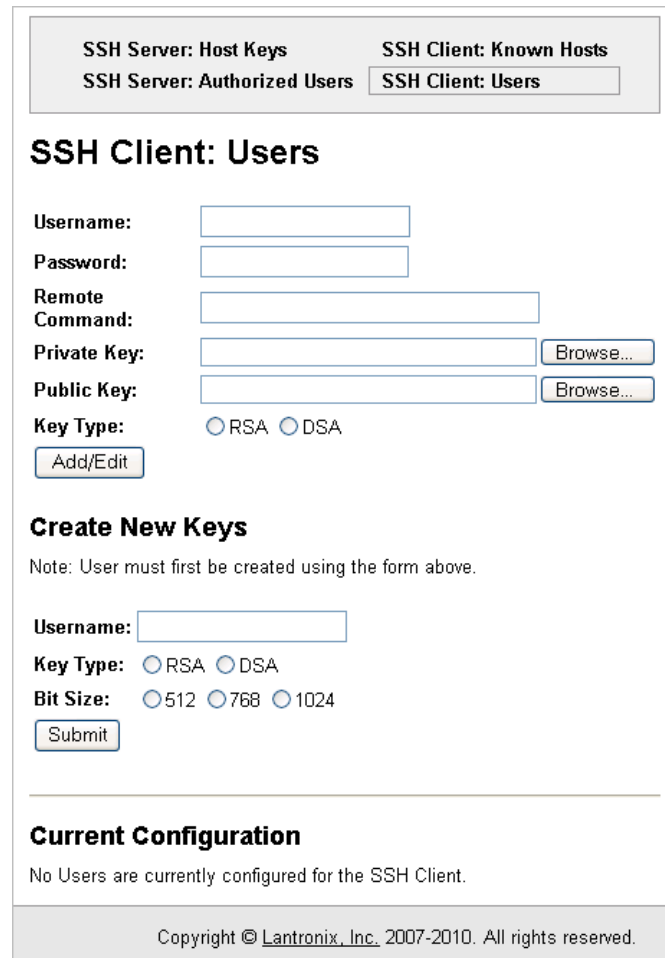
You can configure SSH client settings for users. SSH client known users are used by all applications that play the role of an SSH client, specifically tunneling in Connect Mode. Minimumally, a password or key pair must be configured for a user.

The keys for public key authentication can be created on another device and uploaded to the MatchPort AR or automatically generated on the MatchPort AR. If uploading existing keys, be sure the private key does not get compromised in transit. Upload the data over a secure private network. If you are uploading a key, ensure that it is not password protected.

To configure the SSH client users, perform the following steps.

1. Click **SSH > SSH Client Users**. [Figure 10-4](#) shows the page that displays.

Figure 10-4 SSH Client Users Web Page



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

No Users are currently configured for the SSH Client.

Copyright © Lantronix, Inc. 2007-2010. All rights reserved.

2. Enter or modify the fields in [Table 10-4](#).

Table 10-4 SSH Client Users Fields

Field	Description
Username	Enter the name that the MatchPort AR uses to connect to a SSH server.
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 Browse 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 Browse button to select the key.

Table 10-4 SSH Client Users Fields (continued)

Field	Description
Key Type	Select the key type to be used. Choices are: ◆ RSA—Use this key with the SSH1 and SSH2 protocols. ◆ DSA—Use this key with the SSH2 protocol.
Create New Keys	
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: ◆ RSA—Use this key with the SSH1 and SSH2 protocols. ◆ DSA—Use this key with the SSH2 protocol.
Bit Size	Select the bit length of the new key: ◆ 512 ◆ 768 ◆ 1024 Using a larger Bit Size takes more time to generate the key. Approximate times are: ◆ 10 seconds for a 512 bit RSA Key ◆ 15 seconds for a 768 bit RSA Key ◆ 1 minute for a 1024 bit RSA key ◆ 30 seconds for a 512 bit DSA key ◆ 1 minute for a 768 bit DSA key ◆ 2 minutes for a 1024 bit DSA key Note: Some SSH clients require RSA host keys to be at least 1024 bits long.

3. Click **Submit**.

Note: You can delete stored settings when the **[Delete]** link displays in the **Current Configuration** table.

SSL Cipher Suites

The SSL standard defines only certain combinations of certificate type, key exchange method, symmetric encryption, and hash method. Such a combination is called a cipher suite. [Table 10-5](#) lists the supported cipher suites.

Table 10-5 Supported Cipher Suites

Certificate	Key Exchange	Encryption	Hash
DSA	DHE	3DES	SHA1
RSA	RSA	128 bits AES	SHA1
RSA	RSA	Triple DES	SHA1
RSA	RSA	128 bits RC4	MD5

Table 10-5 Supported Cipher Suites (continued)

Certificate	Key Exchange	Encryption	Hash
RSA	RSA	128 bits RC4	SHA1
RSA	1024 bits RSA	56 bits RC4	MD5
RSA	1024 bits RSA	56 bits RC4	SHA1
RSA	1024 bits RSA	40 bits RC4	MD5

Whichever side is acting as server decides which cipher suite to use for a connection. It is usually the strongest common denominator of the cipher suite lists supported by both sides.

SSL Certificates

The goal of a certificate is to authenticate its sender. It is analogous to a paper document that contains personal identification information and is signed by an authority, for example a notary or government agency.

The principles of Security Certificate required that in order to sign other certificates, the authority uses a private key. The published authority certificate contains the matching public key that allows another to verify the signature but not recreate it.

The authority's certificate can be signed by itself, resulting in a self-signed or trusted-root certificate, or by another (higher) authority, resulting in an intermediate authority certificate. You can build up a chain of intermediate authority certificates, and the last certification will always be a trusted-root certificate.

An authority that signs another certificates is also called a Certificate Authority (CA). The last in line is then the root-CA. VeriSign is a famous example of such a root-CA. Its certificate is often built into web browsers to allow verifying the identity of website servers, which need to have certificates signed by VeriSign or another public CA. Since obtaining a certificate signed by a CA that is managed by another company can be expensive, it is possible to have your own CA. Tools exist to generate self-signed CA certificates or to sign other certificates.

A certificate request is a certificate that has not been signed and only contains the identifying information. Signing it makes it a certificate. A certificate is also used to sign any message transmitted to the peer to identify the originator and prevent tampering while transported.

When using HTTPS, SSL Tunneling in Accept mode, and/or EAP-TLS, the MatchPort AR needs a personal certificate with a matching private key to identify itself and sign its messages. When using SSL Tunneling in Connect mode and/or EAP-TLS, EAP-TTLS or PEAP, the MatchPort AR needs the authority certificate that can authenticate users with which it wishes to communicate.

SSL RSA or DSA

As mentioned above, the certificates contain a public key. Different key exchange methods require different public keys and thus different styles of certificate. The MatchPort AR supports key exchange methods that require a RSA-style certificate and key exchange methods that require a DSA-style certificate. If only one of these certificates is stored in the MatchPort AR, only those key exchange methods that can work with that style certificate are enabled. RSA is sufficient in most cases.

SSL Certificates and Private Keys

You can obtain a certificate by completing a certificate request and sending it to a certificate authority that will create a certificate/key combo, usually for a fee. Or generate your own. A few utilities exist to generate self-signed certificates or sign certificate requests. The MatchPort AR also has the ability to generate its own self-signed certificate/key combo.

You can use XML to export the certificate in PEM format, but you cannot export the key. Hence the internal certificate generator can only be used for certificates that are to identify that particular MatchPort AR.

Certificates and private keys can be stored in several file formats. Best known are PKCS12, DER and PEM. Certificate and key can be in the same file or in separate files. The key can be encrypted with a password or not. The MatchPort AR currently only accepts separate PEM files. The key needs to be unencrypted.

SSL Utilities

Several utilities exist to convert between the formats as follows:

- ◆ **OpenSSL**—Open source set of SSL related command line utilities. It can act as server or client. It can generate or sign certificate requests. It can convert all kinds of formats. Executables are available for Linux and Windows. To generate a self-signed RSA certificate/key combo use the following commands in the order shown:

```
openssl req -x509 -nodes -days 365 -newkey rsa:1024 -keyout
mp_key.pem -out mp_cert.pem
```

Note: Signing other certificate requests is also possible with OpenSSL. See www.openssl.org or www.madboa.com/geek/openssl for more information.

- ◆ **Steel Belted Radius**—Commercial radius server by Juniper Networks that provides a GUI administration interface. It also provides a certificate request and self-signed certificate generator. The self-signed certificate has extension .sbrpvk and is in the PKCS12 format. OpenSSL can convert this into a PEM format certificate and key by using the following commands in the order shown:

```
openssl pkcs12 -in sbr_certkey.sbrpvk -nodes -out sbr_certkey.pem
```

The sbr_certkey.pem file contains both certificate and key. If loading the SBR certificate into MatchPort AR as an authority, you will need to edit it. Open the file in any plain text editor. Delete all info before the following:

```
"----- BEGIN CERTIFICATE-----"
```

and after

```
"----- END CERTIFICATE-----"
```

and save as sbr_cert.pem. SBR accepts trusted-root certificates in the DER format. Again, OpenSSL can convert any format into DER by using the following commands in the order shown:

```
openssl x509 -inform pem -in mp_cert.pem -outform der -out
mp_cert.der
```

Note: With SBR, when the identity information includes special characters such as dashes and periods, SBR changes the format it uses to store these strings and becomes incompatible with the current MatchPort AR release. We will add support for this and other formats in future releases.

- ◆ Free Radius—Linux open-source Radius server. It is versatile, but complicated to configure.

SSL Configuration

To configure SSL, perform the following steps.

1. Click **SSL** from the Main Menu. [Figure 10-5](#) shows the page that displays.

Figure 10-5 SSL Web Page

SSL

Upload Certificate

New Certificate:

New Private Key:

Upload Authority Certificate

Authority:

Create New Self-Signed Certificate

Country (2 Letter Code):

State/Province:

Locality (City):

Organization:

Organization Unit:

Common Name:

Expires: mm/dd/yyyy

Key length: ☐ 512 bit ☐ 768 bit ☐ 1024 bit

Type: ☐ RSA ☐ DSA

Current SSL Certificates

<None>

Current Certificate Authorities

<None>

Copyright © Lantronix, Inc. 2007-2010. All rights reserved.

2. Enter or modify the fields in [Table 10-6](#).

Table 10-6 SSL Fields

Field	Description
Upload Certificate	
New Certificate	This certificate identifies the MatchPort AR to peers. It is used for HTTPS and SSL Tunneling. Enter the path and name of the certificate you want to upload, or use the Browse button to select the certificate. RSA or DSA certificates with 512 to 1024 bit public keys are allowed. Note: The file format must be PEM. The file must start with "-----BEGIN CERTIFICATE-----" and end with "-----END CERTIFICATE-----". Some Certificate Authorities add comments before and/or after these lines. Those need to be deleted before upload.
New Private Key	Enter the path and name of the private key you want to upload, or use the Browse button to select the private key. The key needs to belong to the certificate entered above. Note: The format of the file must be PEM. The file must start with "-----BEGIN RSA PRIVATE KEY-----" and end with "-----END RSA PRIVATE KEY-----". Read DSA instead of RSA in case of a DSA key. Some Certificate Authorities add comments before and/or after these lines. Those need to be deleted before upload.
Upload Authority Key	
Authority	One or more authority certificates are needed to verify a peer's identity. It is used for SSL Tunneling. These certificates do not require a private key. Enter the path and name of the certificate you want to upload, or use the Browse button to select the certificate. RSA or DSA certificates with 512 to 1024 bit public keys are allowed. Note: The format of the file must be PEM. The file must start with "-----BEGIN CERTIFICATE-----" and end with "-----END CERTIFICATE-----". Some Certificate Authorities add comments before and/or after these lines. Those need to be deleted before upload.
Create New Self-Signed Certificate	
Country	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	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. Example: 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. Example: If your company is setting up a web server for the Sales department, enter Sales for your organizational unit.
Expires	Enter the expiration date, in mm/dd/yyyy format, for the new self-signed certificate. Example: An expiration date of May 9, 2010 is entered as 05/09/2010.

Table 10-6 SSL Fields (continued)

Field	Description
Key Length	Select the bit size of the new self-signed certificate. Choices are: ◆ 512 bits ◆ 768 bits ◆ 1024 bits The larger the bit size, the longer it takes to generate the key. Approximate times are: ◆ 10 seconds for a 512-bit RSA key ◆ 30 seconds for a 768-bit RSA key ◆ 1 minute for a 1024-bit RSA key ◆ 30 seconds for a 512-bit DSA key ◆ 2 minutes for a 768-bit DSA key ◆ 6 minute for a 1024-bit DSA key
Type	Select the type of key: ◆ RSA—Public-Key Cryptography algorithm based on large prime numbers, invented by Rivest Shamir and Adleman. Used for encryption and signing. ◆ DSA—Digital Signature Algorithm also based on large prime numbers, but can only be used for signing. Developed by the US government to avoid the patents on RSA.

11: VIP

VIP (Virtual IP) takes advantage of the Lantronix ManageLinux technology that solves the access-through-firewall problem. ManageLinux utilizes existing network infrastructure to create a virtual device network (VDN).

VDN provides direct access to only authorized equipment, behind firewalls, from anywhere via the net. The VDN technology enables you to create dedicated TCP/IP connections between any two devices, using easily deployed hardware appliances. There is no client software to install. No changes are required to network software or applications at either end of the connection.

ManageLinux is a secure and totally transparent remote access solution. The VDN hardware consists of a publicly accessible Device Services Manager (DSM) and individual Device Services Controller (DSC) appliances in multiple locations. Together, these two components enable you to set up and manage individual Virtual IP (VIP) addresses and routes.

The MatchPort AR with VIP enabled takes the place of a DSC and provides direct access to your equipment.

The MatchPort AR supports both Accept and Connect Mode tunneling through VIPs. Configuring an MatchPort AR to use VIP Access involves:

- ◆ Obtaining a ManageLinux XML bootstrap file
- ◆ Importing the ManageLinux XML bootstrap file
- ◆ Enabling VIP access
- ◆ Configuring your tunnels to use the VIPs

Once the MatchPort AR is configured and enabled to use VIPs, it will immediately attempt to establish a conduit with the ManageLinux DSM. Once the conduit is up, tunneling via VIP Access is ready to go.

This chapter contains the following sections:

- ◆ [Obtain a Bootstrap File](#)
- ◆ [Import the Bootstrap File](#)
- ◆ [Enable VIP](#)
- ◆ [Configure Tunnels to Use VIP](#)
- ◆ [VIP Statistics](#)
- ◆ [VIP Configuration](#)

Obtain a Bootstrap File

The ManageLinux XML bootstrap file is an XML file that contains the information required to contact and authenticate to a DSM. This file must be generated and sent to you by the DSM administrator. See the ManageLinux documentation for more details.

Import the Bootstrap File

To configure an MatchPort AR to use VIP Access, import the bootstrap file as you would any XML Configuration Record (XCR). For instructions on importing XCRs, see [Chapter 13: Advanced Settings](#).

Enable VIP

Once the bootstrap file has been imported, VIP Access can be enabled and a conduit with the DSM will be established. The VIP Statistics shows the current state of the conduit. When configured correctly, a conduit with the DSM will be maintained at all times.

Configure Tunnels to Use VIP

Configuring Connect Mode tunnels to use VIP is a simple matter of configuring a tunnel as is normally done, but also enabling VIP in the Tunnel Host settings, and using a VIP Name for the address. VIP Accept Mode tunnels do not require special configuration. If VIP access is enabled (in the VIP configuration page), then VIP Accept Mode requests from a ManageLinx device will be accepted.

VIP Statistics

To view the VIP statistics, click **VIP** from the Main Menu. [Figure 11-1](#) shows the page that displays and [Table 11-1](#) describes the fields.

Figure 11-1 VIP Statistics Web Page

Statistics Configuration	
Virtual IP (VIP) Statistics	
DSM IP Address:	
Local Dna ID:	
Tunnel User:	
Tunnel Port List:	
Current Tunnel Port:	0
Conduit Status:	Down
Conduit Uptime:	0 days 00:00:00
Time of Last Replication:	
Config Name:	
Network Interfaces:	<None>
Copyright © Lantronix, Inc. 2007-2010. All rights reserved.	

Table 11-1 VIP Statistics Fields

Field	Description
DSM IP Address	Address of the Device Services Manager (DSM) from the bootstrap file.
Local DNA ID	Identity of this device from the bootstrap file.
Tunnel User	username of this device from the bootstrap file.
Tunnel Port List	DSM listening ports from the bootstrap file.
Current Tunnel Port	DSM port currently used by the conduit.
Conduit Status	Indicates the status of the secure communications channel to the ManageLinux DSM.
Conduit Uptime	Amount of time the conduit has been established between the MatchPort AR and DSM.
Time of Last Replication	Time and date when configuration information was last received from a ManageLinux DSM.
Config Name	The name used by the ManageLinux DSM to identify the MatchPort AR.
Network Interfaces	VIP names that can be used in Tunnel Connect Mode for a Host.

VIP Configuration

To configure VIP, perform the following steps.

1. Click **VIP > Configuration** from the Main Menu. [Figure 11-2](#) shows the page that displays.

Figure 11-2 VIP Configuration Web Page



Statistics Configuration

Virtual IP (VIP) Configuration

State: ☐ Enabled ☒ Disabled

Copyright © Lantronix, Inc. 2007-2010. All rights reserved.

2. Click **Enabled** to use VIP addresses in Tunnel Accept Mode and Tunnel Connect Mode. The default is disabled.
3. Click **Submit**.

12: Maintenance and Diagnostics Settings

This chapter describes maintenance and diagnostic methods and contains the following sections:

- ◆ [Filesystem](#)
- ◆ [Protocol Stack](#)
- ◆ [IP Address Filter](#)
- ◆ [Query Port](#)
- ◆ [Diagnostics](#)
- ◆ [System](#)

Filesystem

The MatchPort AR uses a flash filesystem to store files. You can view file diagnostics and/or modify files. There are two subsections: Statistics and Browse.

The Statistics section of the Filesystem Statistics window shows current statistics and usage information of the flash file system. In the FileSystem Browser section of the Filesystem Statistics web page, you can create files and folders, upload files, copy and move files, and use TFTP.

Filesystem Statistics and Actions

To display the filesystem statistics, compact, or format the filesystem, perform the following steps.

1. Click **Filesystem** on the Main Menu. [Figure 12-1](#) shows the page that displays.

Figure 12-1 Filesystem Statistics Web Page

Statistics Browse	
Filesystem Statistics	
Filesystem Size:	3.562500 Mbytes (3735552 bytes)
Available Space:	3.559544 Mbytes (3732454 bytes) (99%)
Clean Space:	3.559544 Mbytes (3732454 bytes) (99%)
Dirty Space:	0 bytes (0%)
File & Dir Space Used:	3.025 Kbytes (3098 bytes) (0%)
Data Space Used:	2.750 Kbytes (2817 bytes)
Number of Files:	0
Number of Dirs:	0
Number of System Files:	2
Opened Files:	0
Locked Files:	0
Opened for Sharing:	0
Current Bank:	B
FW Sectors:	02 - 13, 1 erase cycle
Bank A Sectors:	14 - 70, 0 erase cycles
Bank B Sectors:	71 - 127, 2 erase cycles
Busy:	No
Actions:	[Compact] [Format]
Copyright © Lantronix, Inc., 2007-2010. All rights reserved.	

2. Click **Compact** in the **Actions** row to compact the files.

Note: The compact should not be needed under normal circumstances as the system manages this automatically.

3. Back up all files before you perform Step 4, because all user files get erased in that step.
4. Click **Format** in the Actions row. The configuration gets retained.

Filesystem Browser

To browse the filesystem, perform the following steps.

1. Click **Filesystem > Browse**. Figure 12-2 shows the page that displays.

Figure 12-2 Filesystem Browser Web Page

Statistics
Browse

Filesystem Browser

 /

  http

  test.txt 15 bytes

Create

File:

Directory:

Upload File

Copy File

Source:

Destination:

Move

Source:

Destination:

TFTP

Action: ☐ Get ☐ Put

Mode: ☐ ASCII ☐ Binary

Local File:

Remote File:

Host:

Port:

Copyright © Lantronix, Inc. 2007-2010. All rights reserved.

2. Click a filename to view the contents.

- Click the X next to a filename to delete the file and then you can delete the directory. The directory has to be empty before you can delete it.

Note: Changes apply to the current directory view. To make changes within other folders, click the folder or directory and then enter the parameters in the settings listed in [Table 12-1](#).

Files can be copied or moved by using the fields noted in [Table 12-1](#).

Table 12-1 Filesystem Browser Fields

Field	Description
Create	
File	Enter the name of the file you want to create, and then click Create .
Directory	Enter the name of the directory you want to create, and then click Create .
Upload File	Enter the path and name of the file you want to upload by means of HTTP(S) or use the Browse button to select the file, and then click Upload .
Copy File	
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 Copy to copy the file.
Move	
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 Move to move the file.
TFTP	
Action	Select the action that is to be performed via TFTP: Get —A TFTP get command will be executed to store a file locally. Put —A TFTP put command will be executed to send a file on the local file system to a remote location.
Mode	Select a TFTP mode to use. Choices are: ◆ ASCII ◆ Binary
Local File	Enter the name of the local file.
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 on which the specified TFTP get or put command will be performed. Click Transfer to perform the TFTP transfer.

Protocol Stack

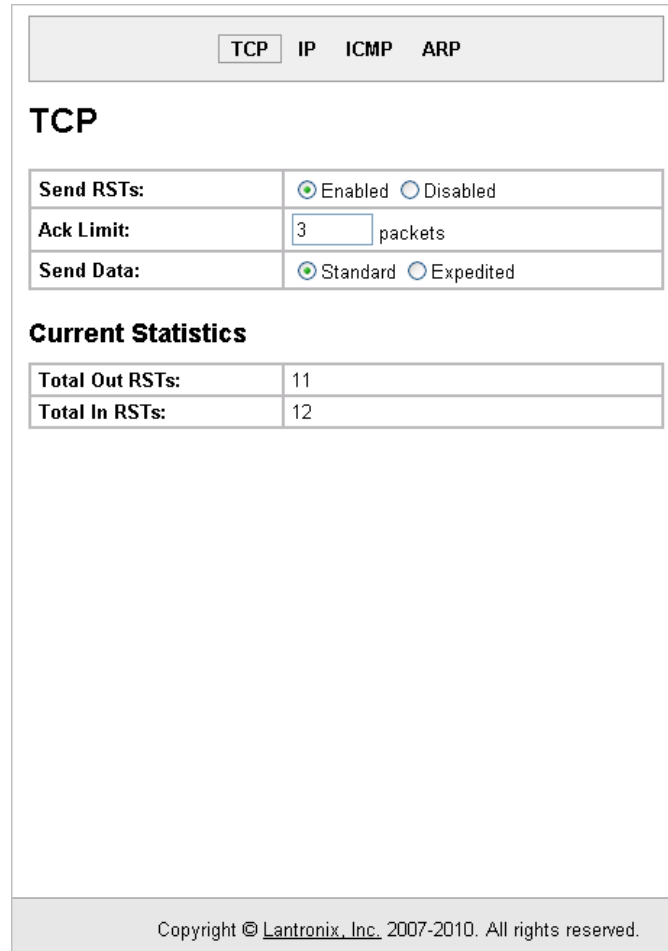
In the Protocol Stack web page, you can configure TCP, IP, ICMP, and ARP.

TCP

To configure the network protocols, perform the following steps.

1. Click **Protocol Stack** on the Main Menu. TCP is the default. [Figure 12-3](#) shows the page that displays.

Figure 12-3 TCP Web Page



2. Enter or modify the fields in [Table 12-2](#).

Table 12-2 TCP Fields

Field	Description
Send RSTs	Click Enabled to send RSTs or Disabled to stop sending RSTs. TCP contains six control bits, with one or more defined in each packet. RST is one of the control bits. The RST bit is responsible for telling the receiving TCP stack to end a connection immediately. Caution: <i>Setting the RSTs may pose a security risk.</i>

Table 12-2 TCP Fields (continued)

Field	Description
Ack Limit	Enter a number to limit how many packets get received before an ACK gets forced. If there is a large amount of data to acknowledge, an ACK gets forced. If the sender TCP implementation waits for an ACK before sending more data even though the window is open, setting the Ack Limit to 1 packet improves performance by forcing immediate acknowledgements.
Send Data	The Send Data selection governs when data may be sent into the network. The Standard implementation waits for an ACK before sending a packet less than the maximum length. Select Expedited to send data whenever the window allows it.

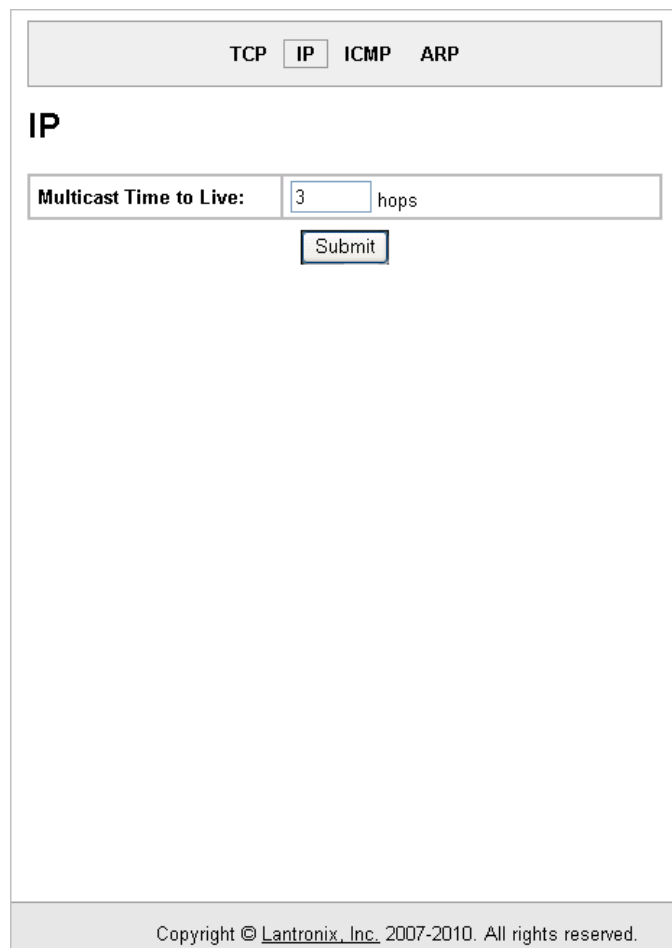
3. Click **Submit**.

IP

To change the IP settings, perform the following steps.

1. Click **Protocol Stack > IP**. Figure 12-4 shows the page that displays.

Figure 12-4 IP Web Page



TCP **IP** ICMP ARP

IP

Multicast Time to Live: hops

Copyright © Lantronix, Inc. 2007-2010. All rights reserved.

2. Enter the number of hops a multicast packet can complete before it is terminated as a Multicast Time to Live.
3. Click **Submit**.

ICMP

To set the ICMP, perform the following steps.

1. Click **Protocol Stack > ICMP**. [Figure 12-5](#) shows the page that displays.

Figure 12-5 ICMP Web Page



The screenshot shows a web interface for configuring ICMP. At the top, there is a navigation bar with tabs for TCP, IP, ICMP (which is selected), and ARP. Below the navigation bar, the title "ICMP" is displayed. Underneath the title, there is a "State:" label followed by two radio button options: "Enabled" and "Disabled". The "Enabled" radio button is selected. Below these options is a "Submit" button. At the bottom of the page, there is a copyright notice: "Copyright © Lantronix, Inc. 2007-2010. All rights reserved."

2. Click **Enabled**.
3. Click **Submit**.

ARP

1. Click **Protocol Stack > ARP**. Figure 12-6 shows the page that displays.

Figure 12-6 ARP Web Page

TCP IP ICMP **ARP**

ARP

ARP Timeout: hours
 minutes
 seconds

ARP Cache

IP Address:
 MAC Address:

Current State [Remove All]

Address	Age Sec	MAC Address	Type	Interface
172.19.1.1 [Remove]	9.6	00:1b:21:0e:3d:f4	Dynamic	1
172.19.100.79 [Remove]	0.0	00:25:11:3f:47:4d	Dynamic	1

Copyright © Lantronix, Inc. 2007-2010. All rights reserved.

1. Enter the fields in Table 12-3.

Table 12-3 ARP Web Page Fields

Field	Description
ARP	
ARP Timeout	Enter hours, minutes and seconds. This is the maximum duration an address remains in the cache.
ARP Cache	
IP Address	Enter the IP address for the ARP cache.
MAC Address	Enter the MAC address to add to the ARP cache.
Current State [Remove All]	Removes all entries in the ARP cache or click [Remove] in the specific table entry to remove that entry.

2. Click **Submit** for ARP or click **Add** for ARP Cache.

Note: Both the IP and MAC addresses are required for the ARP cache.

IP Address Filter

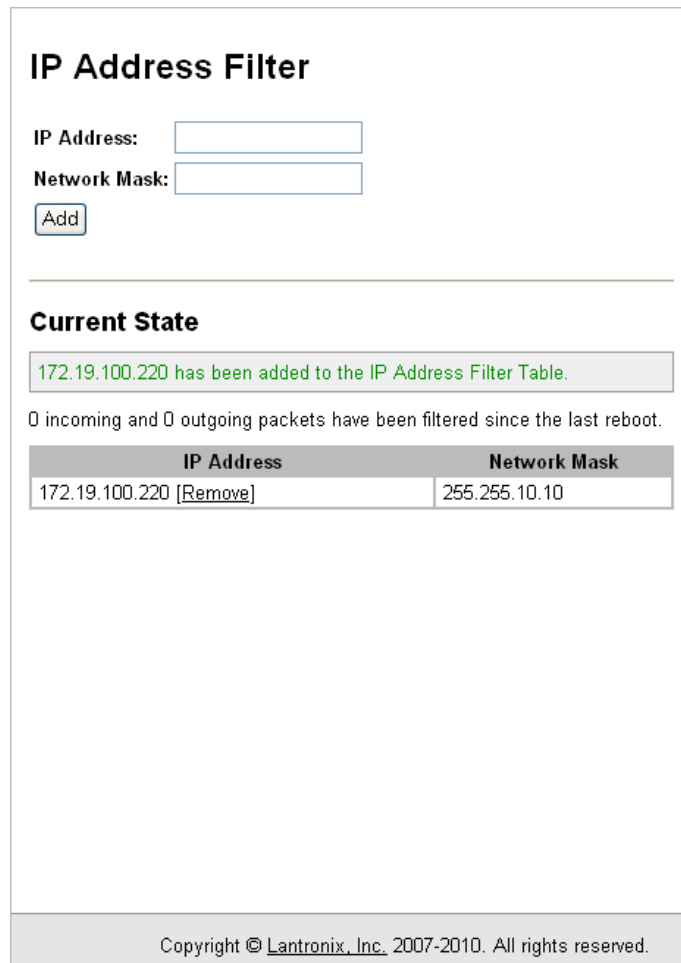
The IP address filter allows specified hosts and subnets to communicate with the MatchPort AR.

Note: If using DHCP/BOOTP, ensure the DHCP/BOOTP server IP address is in the list.

To configure the IP address filter, perform the following steps.

1. Click the **IP Address Filter** on the Main Menu. [Figure 12-7](#) shows the page that displays.

Figure 12-7 IP Address Filter Web Page



IP Address Filter

IP Address:

Network Mask:

Current State

172.19.100.220 has been added to the IP Address Filter Table.

0 incoming and 0 outgoing packets have been filtered since the last reboot.

IP Address	Network Mask
172.19.100.220 [Remove]	255.255.10.10

Copyright © Lantronix, Inc. 2007-2010. All rights reserved.

Note: Be aware not to assign your network IP address as “filtered.” You will have to reset your system because the MatchPort AR has locked your network out.

2. Enter or modify the fields in [Table 12-4](#).

Table 12-4 IP Address Filter Fields

Field	Description
IP Address	Enter the IP address to add to the IP filter table.

Table 12-4 IP Address Filter Fields (continued)

Field	Description
Network Mask	Enter the IP address' network mask in dotted notation.

- Click **Add**.

Note: You can remove IP addresses by clicking **[Remove]** in the **Current State** table.

Query Port

The query port (0x77FE) is used for the automatic discovery of the device by the DeviceInstaller utility. Only 0x77FE discover messages from DeviceInstaller are supported. For more information on DeviceInstaller, see [3: Using DeviceInstaller](#)

To configure the query port server, perform the following steps.

- Click **Query Port** on the Main Menu. [Figure 12-8](#) shows the page that displays.

Figure 12-8 Query Port Web Page

Query Port

Query Port Server: ☒ On ☐ Off

Current Configuration and Statistics

Query Port Status:	On (running)
In Valid Queries:	0
In Unknown Queries:	0
In Erroneous Packets:	0
Out Query Replies:	0
Out Errors:	0
Last Connection:	No device has connected

Copyright © Lantronix, Inc. 2007-2010. All rights reserved.

- Select **On**. Off is the default.
- Click **Submit**.

Diagnostics

The MatchPort AR has several tools to perform diagnostics and view device statistics. These include information on:

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

Hardware

To display the Hardware configuration, perform the following steps.

1. Click **Diagnostics > Hardware**. [Figure 12-9](#) shows the page that displays.

Figure 12-9 Diagnostics Hardware Web Page

Hardware
MIB-II
IP Sockets

Ping
Traceroute
DNS Lookup

Memory
Buffer Pools
Processes

Diagnostics: Hardware

Current Configuration

CPU Type:	DSTniFX
CPU Speed:	166.666666 MHz
CPU Instruction Cache:	4.000 Kbytes (4096 bytes)
CPU Data Cache:	4.000 Kbytes (4096 bytes)
RAM Size:	8.000000 Mbytes (8388608 bytes)
Flash Size:	8.000000 Mbytes (8388608 bytes)
Flash Sector Size:	64.000 Kbytes (65536 bytes)
Flash Sector Count:	128
Flash ID:	0x20

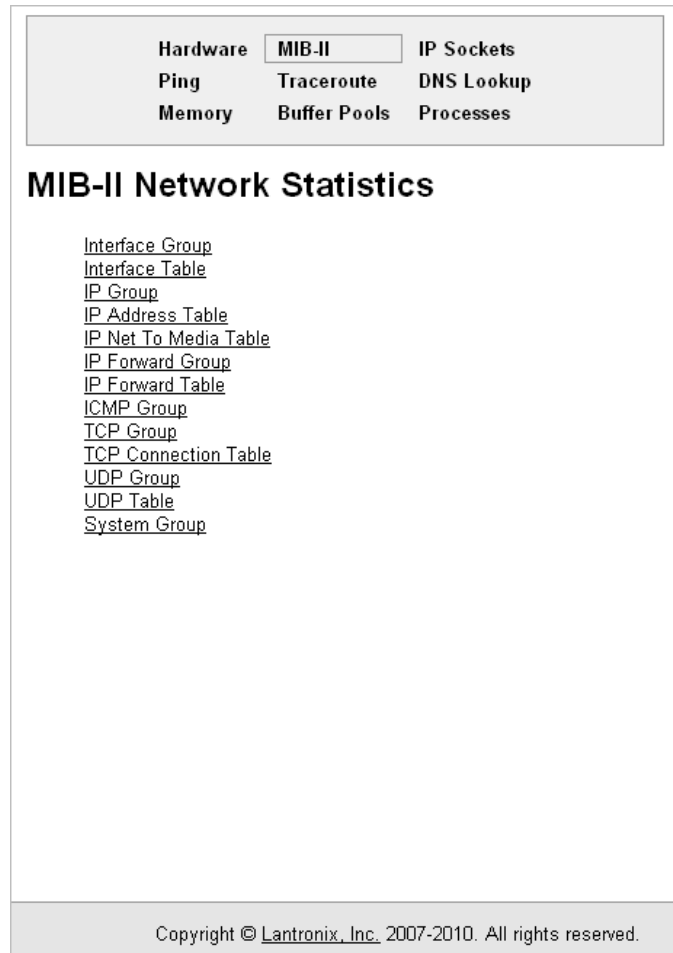
Copyright © Lantronix, Inc. 2007-2010. All rights reserved.

MIB-II

The MIB-II Network Statistics page shows the available SNMP MIBs. To display MIB-II statistics, perform the following steps.

1. Click **Diagnostics > MIB-II** at the top of the page. [Figure 12-10](#) shows the page that displays.

Figure 12-10 MIB-II Network Statistics Web Page



2. Click any of the links to open the corresponding table and statistics.

Note: For more information, refer to the following Requests for Comments (RFCs):

- ◆ RFC 1213—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.

IP Sockets

To display all open IP sockets, perform the following steps.

1. Click **Diagnostics > IP Sockets**. [Figure 12-11](#) shows the page that displays.

Figure 12-11 IP Sockets Web Page

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

IP Sockets

Protocol	RxQ	TxQ	LocalAddr:Port	RemoteAddr:Port	State
UDP	0	0	172.19.100.220:161	255.255.255.255:0	
TCP	0	0	172.19.100.220:21	255.255.255.255:0	LISTEN
UDP	0	0	172.19.100.220:69	255.255.255.255:0	
TCP	0	0	172.19.100.220:80	255.255.255.255:0	LISTEN
UDP	0	0	172.19.100.220:30718	255.255.255.255:0	
TCP	0	0	172.19.100.220:23	255.255.255.255:0	LISTEN
TCP	0	0	172.19.100.220:22	255.255.255.255:0	LISTEN
TCP	0	0	172.19.100.220:10002	255.255.255.255:0	LISTEN
TCP	0	0	172.19.100.220:10001	255.255.255.255:0	LISTEN
TCP	0	4	172.19.100.220:80	172.19.100.79:1463	ESTABLISHED

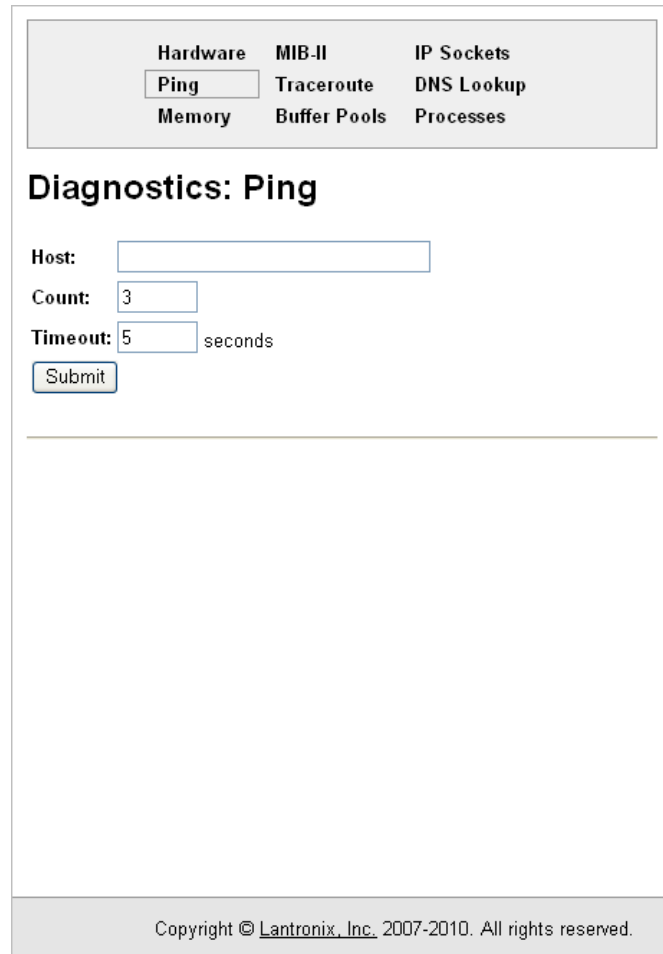
Copyright © Lantronix, Inc. 2007-2010. All rights reserved.

Ping

To ping a remote device or computer, perform the following steps.

1. Click **Diagnostics > Ping**. [Figure 12-12](#) shows the page that displays.

Figure 12-12 Ping Web Page



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

Diagnostics: Ping

Host:

Count:

Timeout: seconds

Copyright © Lantronix, Inc. 2007-2010. All rights reserved.

2. Enter or modify the fields in [Table 12-5](#).

Table 12-5 Ping Fields

Field	Description
Host	Enter the IP address or host name for the MatchPort AR to ping.
Count	Enter the number of ping packets MatchPort AR should attempt to send to the Host . The default is 3 .
Timeout	Enter the time, in seconds, for the MatchPort AR to wait for a response from the host before timing out. The default is 5 seconds.

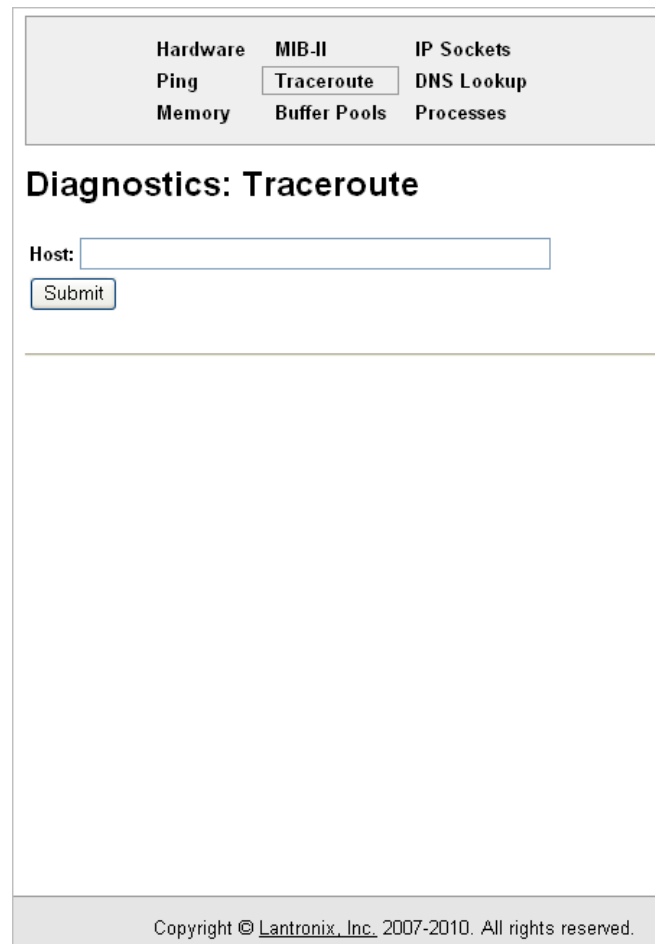
3. Click **Submit**.

Traceroute

You can trace a packet route from the MatchPort AR 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. To use traceroute, perform the following steps.

1. Click **Diagnostics > Traceroute**. [Figure 12-13](#) shows the page that displays.

Figure 12-13 Traceroute Web Page



2. Enter or modify the fields in [Table 12-6](#).

Table 12-6 Traceroute Fields

Field	Description
Host	Enter the IP address or DNS hostname. This address is used to show the path between it and the MatchPort AR when issuing the traceroute command.
Count	Enter the number of ping packets MatchPort AR should attempt to send to the Host. The default is 3 attempts.
Timeout	Enter the time, in seconds, for the MatchPort AR to wait for a response from the host before timing out. The default is 5 seconds.

3. Click **Submit**.

DNS Lookup

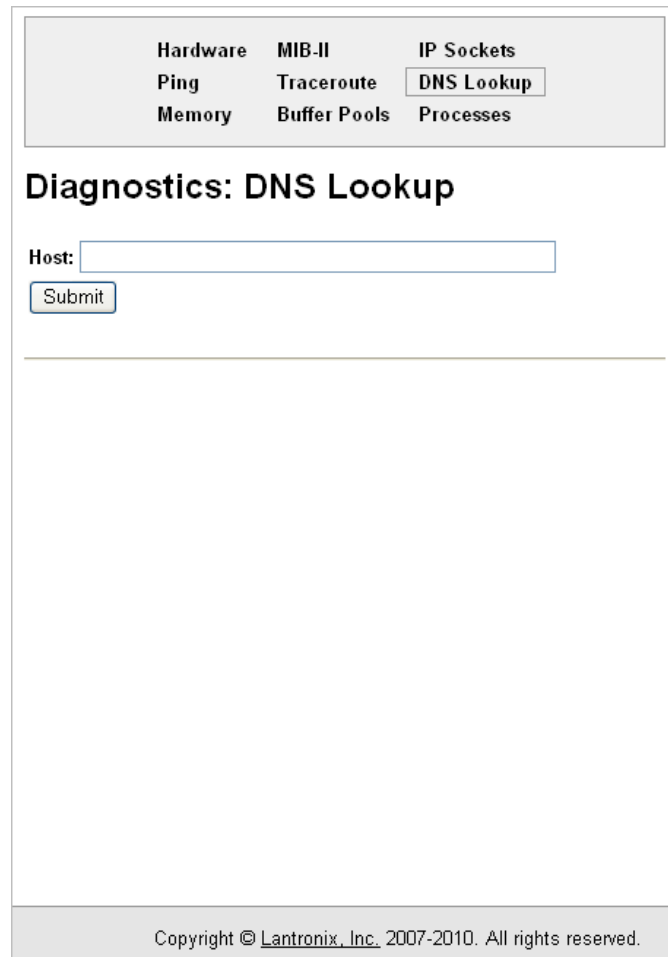
You can specify a DNS Hostname for a forward lookup or an IP address for a reverse lookup. You can also perform a lookup for a Mail (MX) record by prefixing a DNS Hostname with @.

Note: A DNS server must be configured for DNS Lookup to work.

To use forward or reverse DNS lookup, perform the following steps.

1. Click **Diagnostics < DNS Lookup**. [Figure 12-14](#) shows the page that displays.

Figure 12-14 DNS Lookup Web Page



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

Diagnostics: DNS Lookup

Host:

Copyright © Lantronix, Inc. 2007-2010. All rights reserved.

2. Enter or modify the fields in [Table 12-7](#).

Table 12-7 DNS Lookup Fields

Field	Description
Host	Perform one of the following: ◆ For reverse lookup to locate the hostname for that IP address, enter an IP address. ◆ For forward lookup to locate the corresponding IP address, enter a hostname. ◆ To look up the Mail Exchange (MX) record IP address, enter a domain name prefixed with @.

3. Click **Submit**.

Memory

The Memory web page displays total and available memory in bytes, along with the number of fragments, allocated blocks, and memory status. To display memory statistics, perform the following steps.

1. Click **Diagnostics > Memory**. Figure 12-15 shows the page that displays.

Figure 12-15 Memory Web Page

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

Diagnostics: Memory

	Main Heap
Total Memory (bytes):	4160224
Available Memory (bytes):	881760
Number Of Fragments:	5
Largest Fragment Avail:	869216
Allocated Blocks:	2412
Number Of Allocs Failed:	0
Status	OK

Copyright © Lantronix, Inc. 2007-2010. All rights reserved.

Buffer Pools

Private buffer pools ensure deterministic memory management. To display the buffer pools, perform the following steps.

1. Click **Diagnostics > Buffer Pools**. [Figure 12-16](#) shows the page that displays.

Figure 12-16 Buffer Pools Web Page

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	11
Cluster Pool Size: 2048	256	254	2	7

Ethernet Driver Buffer Pool				
	Total	Free	Used	MaxUsed
Buffer Headers	2048	1984	64	70
Cluster Pool Size: 2048	1024	960	64	69

Serial Driver Line 1 Buffer Pool				
	Total	Free	Used	MaxUsed
Buffer Headers	12	6	6	6
Cluster Pool Size: 1024	6	0	6	6

Serial Driver Line 2 Buffer Pool				
	Total	Free	Used	MaxUsed
Buffer Headers	12	6	6	6
Cluster Pool Size: 1024	6	0	6	6

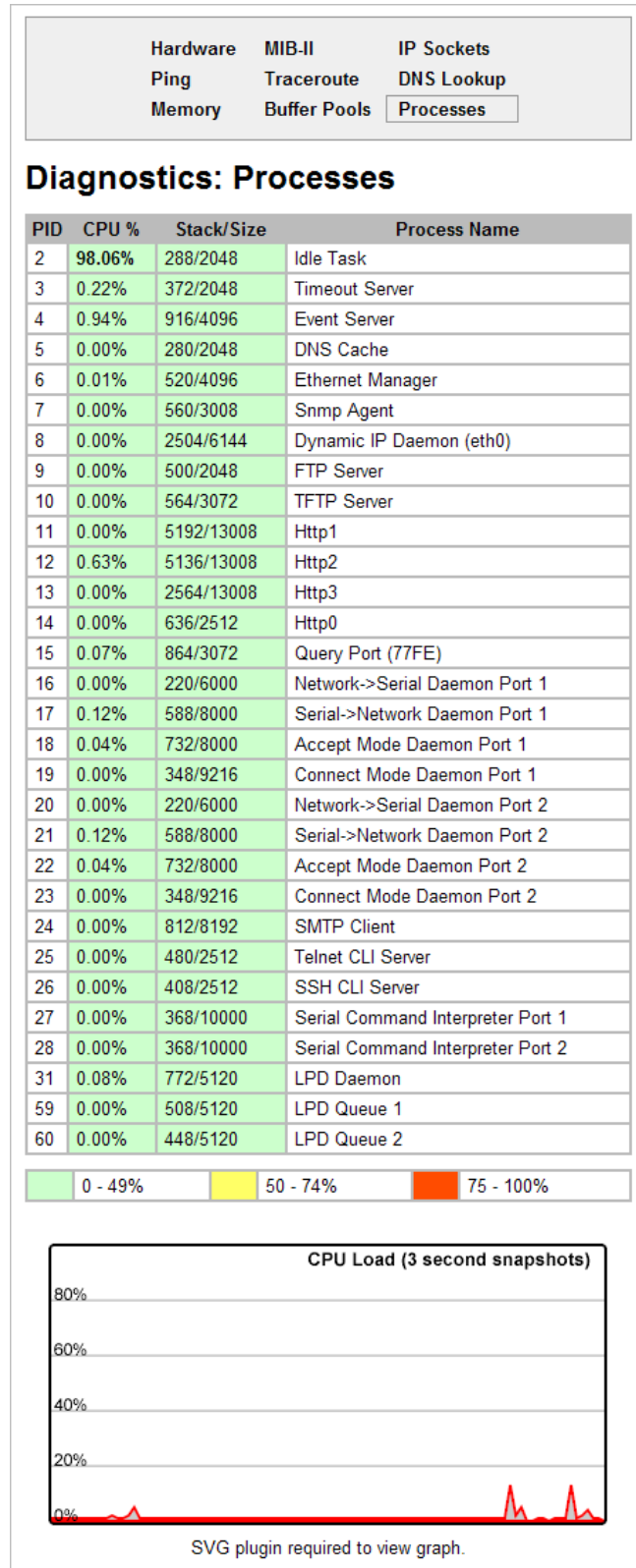
Copyright © [Lantronix, Inc.](#) 2007-2010. All rights reserved.

Processes

The Processes web page shows all the processes currently running on the system. It shows the Process ID (PID), the percentage of total CPU cycles a process used within the last three seconds, the total stack space available, the maximum amount of stack space used by the process since it started, and the process name. To display the processes, perform the following steps.

1. Click **Diagnostics > Processes**. [Figure 12-17](#) shows the page that displays.

Figure 12-17 Processes Web Page



Note: The Adobe SVG plug-in is required to view the CPU Load Graph.

System

The System web page enables the rebooting of the device, restoring factory defaults, uploading new firmware, specifying the short and long name, and viewing the current system configuration.

To configure system settings, perform the following steps.

1. Click **System** on the Main Menu. [Figure 12-18](#) shows the page that displays.

Figure 12-18 System Web Page

The screenshot shows the 'System' web page with the following sections:

- System** (Section Header)
- Reboot Device**
 - Reboot button
- Restore Factory Defaults**
 - Factory Defaults button
- Upload New Firmware**
 - Firmware file input field with a 'Browse...' button
 - Upload button
- Name**
 - Short Name: input field
 - Long Name: input field
 - Submit button
- Current Configuration**

Firmware Version:	5.1.0.0R7
Short Name:	EDS2100
Long Name:	Lantronix EDS2100

Copyright © Lantronix, Inc. 2007-2010. All rights reserved.

2. Enter or modify the fields in [Table 12-8](#).

Table 12-8 System Fields

Field	Description
Reboot Device	Click Reboot to reboot the system. The system refreshes and redirects the browser to the home page.

Table 12-8 System Fields (continued)

Field	Description
Restore Factory Defaults	Click Factory Defaults to restore the MatchPort AR to the original factory settings. All configurations will be lost. The MatchPort AR automatically reboots upon setting back to the defaults.
Upload New Firmware	Click Browse to locate the firmware file location. Click Upload to install the firmware on the MatchPort AR. The device automatically reboots upon the installation of new firmware.
Name	Enter a new Short Name and a Long Name (if necessary). The Short Name maximum is 32 characters. The Long Name maximum is 64 characters. Changes take place upon the next reboot.

3. Click **Submit**.

13: Advanced Settings

This chapter describes the advanced configuration of Email, CLI, and XML. It contains the following sections:

- ◆ [Email Statistics](#)
- ◆ [Email Configuration](#)
- ◆ [Command Line Interface](#)
- ◆ [XML Configuration](#)

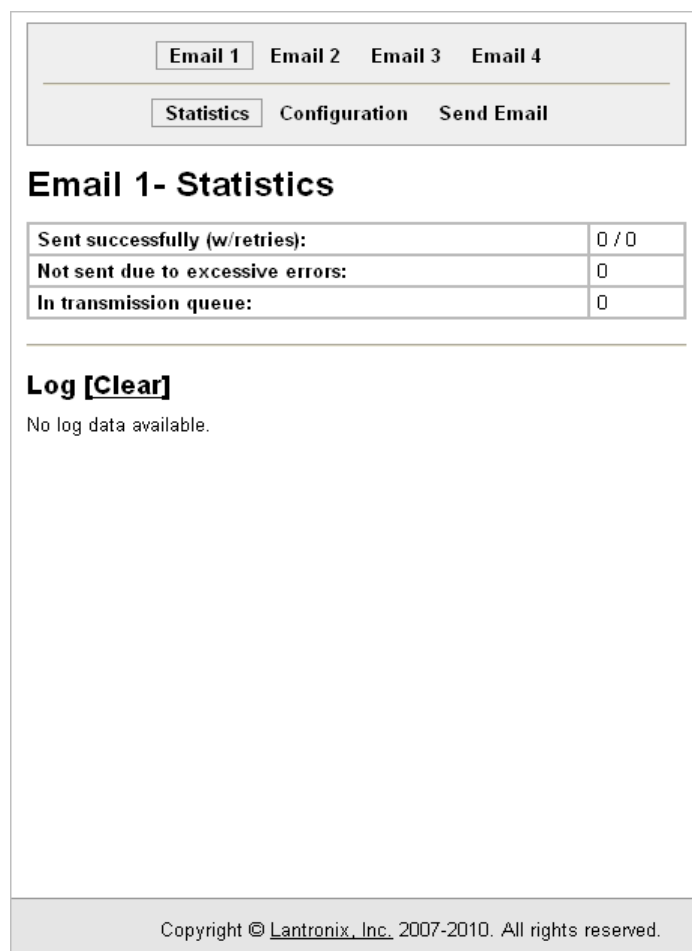
Email Statistics

The Email Statistics web page displays when you click Email from the Main Menu. It shows statistics and current usage information about the email subsystem. When you transmit an email, the transmission to the SMTP server gets logged and displayed in the bottom portion of the page.

To view the statistics, perform the following steps.

1. Click **Email** on the Main Menu. [Figure 13-1](#) shows the page that displays.

Figure 13-1 Email Statistics Web Page



Email 1	Email 2	Email 3	Email 4
Statistics	Configuration	Send Email	

Email 1- Statistics

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

Log [Clear]

No log data available.

Copyright © Lantronix, Inc. 2007-2010. All rights reserved.

2. Click the **Log** [\[Clear\]](#) link to clear the log.

Email Configuration

The MatchPort AR allows you to view and configure email alerts relating to the events occurring within the system. To configure email settings, perform the following steps.

1. Click **Email > Email 1 > Configuration**. [Figure 13-2](#) shows the page that displays.

Figure 13-2 Email 1 Configuration Web Page

Email 1
Email 2
Email 3
Email 4

Statistics
Configuration
Send 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
CP Group:
Trigger Email Send: Value:

Current Configuration

To:	<None>
Cc:	<None>
From:	<None>
Reply-To:	<None>
Subject:	<None>
File:	<None>
Overriding Domain:	<None>
Server Port:	25
Local Port:	<Random> [Delete]
Priority:	Urgent
Trigger Email Send:	Disabled

Copyright © Lantronix, Inc. 2007-2010. All rights reserved.

2. Enter or modify the fields in [Table 13-1](#).

Table 13-1 Email 1 Configuration Fields

Field	Description
To	Enter the email address to which the email alerts will be sent. Multiple addresses are separated by semicolon (;).
Cc	Enter the email address to which the email alerts will be copied. Multiple addresses are separated by semicolon (;).
From	Enter the email address to list in the From field of the email alert.
Reply-To	Enter the email address to list in the Reply-To field of the email alert.
Subject	Enter the subject for the email alert.
File	Enter the path of the file to send with the email alert. This file appears within the message body of the email.
Overriding Domain	Enter the domain name to override the current domain name in EHLO (Extended Hello).
Server Port	Enter the SMTP server port number. The default is port 25 .
Local Port	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.
Trigger Email Send	Configure this field to send an email based on a CP Group trigger. The MatchPort AR sends an email when the specified Value matches the specified CP Group's value.

3. Click **Submit**.
4. Test your configuration by sending an email by clicking **Send Email**. Return to the **Statistics** web page for a log of the transmission.

Note: You can delete stored settings in the **Current Configuration** table by clicking on the [\[Delete\]](#) link.

Command Line Interface

The Command Line Interface (CLI) web page enables you to view statistics about the CLI servers listening on the Telnet and SSH ports and to configure CLI settings. When a connection is active, the following display:

- ◆ Remote client information
- ◆ Number of bytes that have been sent and received
- ◆ Kill link to terminate the connection

CLI Statistics

To view the CLI Statistics, perform the following steps.

1. Click **CLI** on the Main Menu. [Figure 13-3](#) shows the page that displays.

Figure 13-3 CLI Statistics Web Page

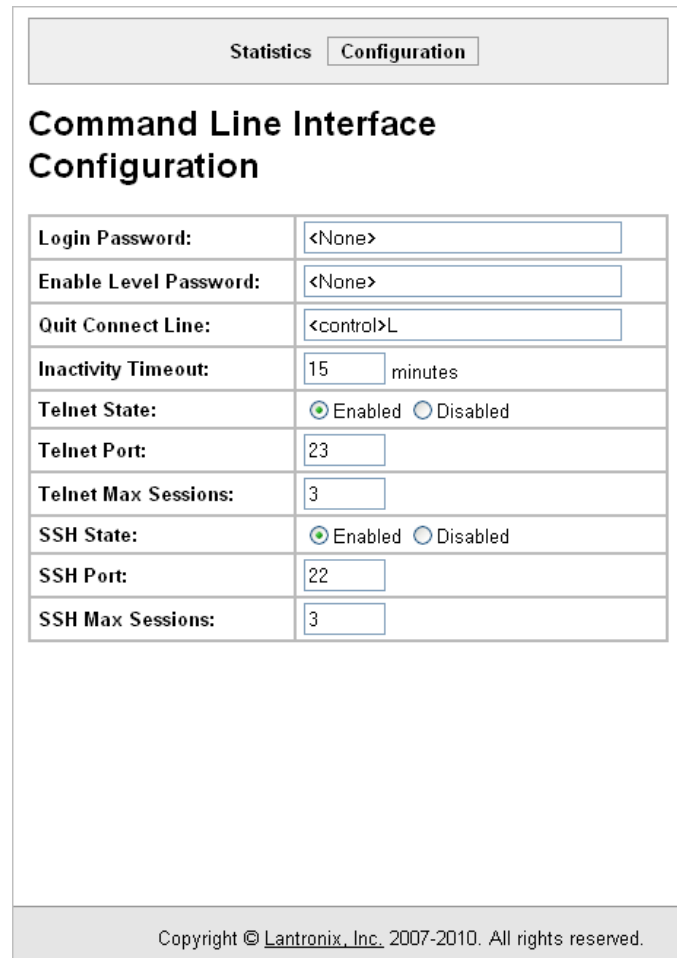
Statistics Configuration	
Command Line Interface Statistics	
Telnet	
Server Status:	Waiting
Last Connection:	<None>
Uptime:	4 days 18:56:17
Total Bytes In:	0
Total Bytes Out:	0
Current Connections:	<None>
SSH	
Server Status:	Waiting
Last Connection:	<None>
Uptime:	4 days 18:56:17
Total Bytes In:	0
Total Bytes Out:	0
Current Connections:	<None>
Copyright © Lantronix, Inc. 2007-2010. All rights reserved.	

CLI Configuration

To configure the CLI, perform the following steps.

1. Click **CLI > Configuration**. [Figure 13-4](#) shows the page that displays.

Figure 13-4 CLI Configuration Web Page



Statistics Configuration	
Command Line Interface Configuration	
Login Password:	<None>
Enable Level Password:	<None>
Quit Connect Line:	<control>L
Inactivity Timeout:	15 minutes
Telnet State:	☒ Enabled ☐ Disabled
Telnet Port:	23
Telnet Max Sessions:	3
SSH State:	☒ Enabled ☐ Disabled
SSH Port:	22
SSH Max Sessions:	3
Copyright © Lantronix, Inc. 2007-2010. All rights reserved.	

2. Enter or modify the fields in [Table 13-2](#).

Table 13-2 CLI Configuration Fields

Field	Description
Login Password	Enter the password for Telnet access.
Enable Level Password	Enter the password for access to the Command Mode Enable level. There is no password by default.
Quit connect line	Enter a string to terminate a connect line session and resume the CLI. Type <control> before any key the user must press when holding down the Ctrl key. An example of such a string is <control>L .
Inactivity Timeout	Set an Inactivity Timeout value so the CLI session will disconnect if no data is received after the designated time period. Default is 15 minutes. Enter a value of 0 to disable.
Telnet State	Select Disabled to disable Telnet access. Telnet is enabled by default.
Telnet Port	Enter the Telnet port to use for Telnet access. The default is 23 .

Table 13-2 CLI Configuration Fields (continued)

Field	Description
Telnet Max Sessions	Maximum number of simultaneous Telnet sessions.
SSH State	Select Disabled to disable SSH access. SSH is enabled by default.
SSH Port	Enter the SSH port to use for SSH access. The default is 22 .
SSH Max Sessions	Maximum number of simultaneous SSH sessions.

3. Click **Submit**.

XML Configuration

The MatchPort AR enables configuration of devices by using XML configuration records (XCRs). You can export an existing configuration for use on other MatchPort ARs or import a saved configuration file.

On the XML: Export Configuration web page, 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 MatchPort AR unit or another. The XML data can be exported to the browser window or to a file on the file system.

By default, all groups are selected except those pertaining to the network configuration (Ethernet and WLAN). This is so that if you later import the entire XML configuration, it will not break your network connectivity. You may select or clear the checkbox for any group.

In the XML: Import System Configuration Page you can import a system configuration from an XML file. The XML data can be imported from a file on the file system 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>;...
```

For example, if you only wanted to import the line 1 setting from an XCR, use a filter string of line:1.

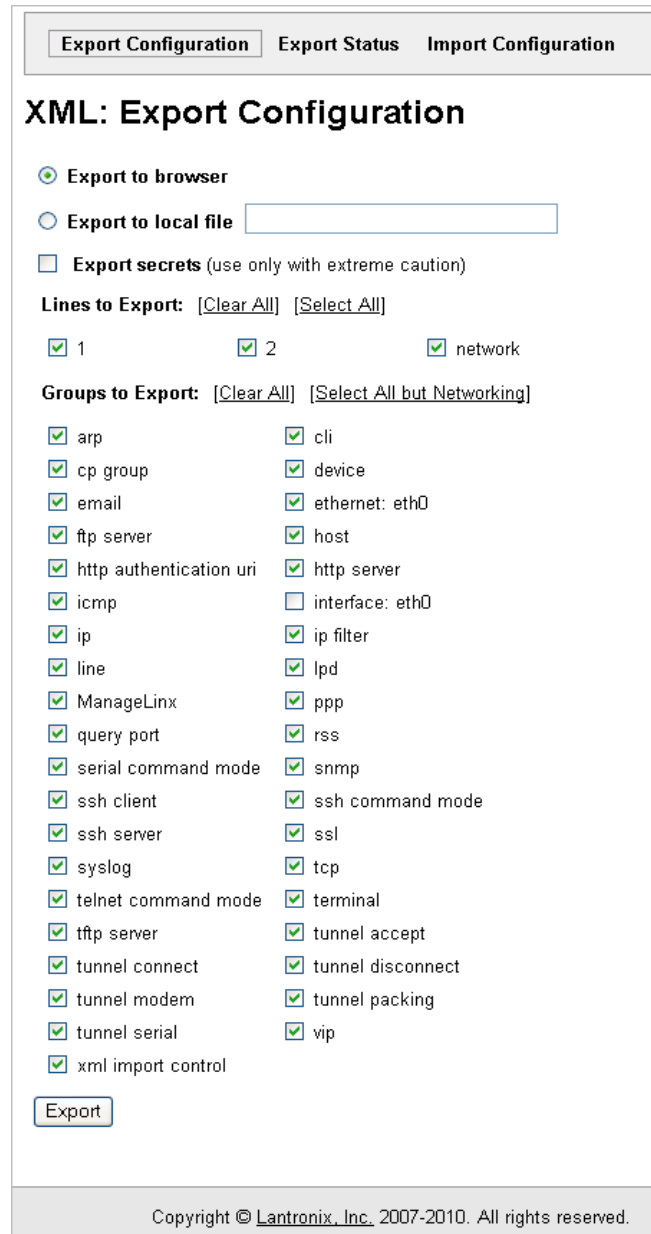
Each group name <g> is followed by a colon and the instance value <i>. Each <g> :<i> value is separated with a semicolon. If a group has no instance, specify the group name <g> only.

XML Export Configuration

To export a system configuration record, perform the following steps.

1. Click **XML** on the Main Menu. [Figure 13-5](#) shows the page that displays.

Figure 13-5 XML Export Configuration Web Page



2. Enter or modify the fields in [Table 13-3](#).

Table 13-3 XML Export Configuration Fields

Field	Description
Export to browser	Select this option to export the XCR data in the selected fields to a web browser.
Export to local file	Select this option to export the XCR data to a file on the device. If you select this option, enter a file name for the XML configuration record.

Table 13-3 XML Export Configuration Fields (continued)

Field	Description
Export secrets	Only use this with extreme caution. If selected, secret password and key information will be exported. Use only with a secure link, and save only in secure locations.
Lines to Export	Select the instances you want to export in the line, LPD, PPP, tunnel, and terminal groups.
Groups to Export	Check the configuration groups that are to be exported to the XML configuration record.

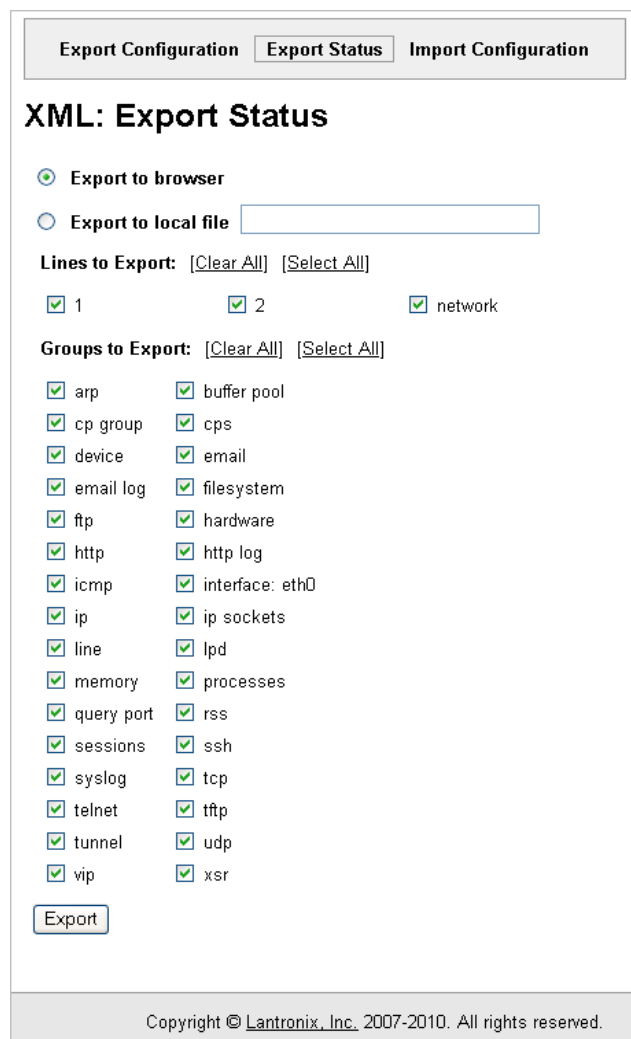
- Click Export. The groups display if exporting to the browser. If exporting to the file system, the MatchPort AR requests a filename for the XML configuration record.

XML Export Status

To export system status in XML format, perform the following steps.

- Click **XML > Export Status**. Figure 13-6 shows the page that displays.

Figure 13-6 XML Export Status Web Page



Export Configuration **Export Status** Import Configuration

XML: Export Status

☒ Export to browser
☐ Export to local file

Lines to Export: [\[Clear All\]](#) [\[Select All\]](#)

☒ 1 ☒ 2 ☒ network

Groups to Export: [\[Clear All\]](#) [\[Select All\]](#)

☒ arp	☒ buffer pool
☒ cp group	☒ cps
☒ device	☒ email
☒ email log	☒ filesystem
☒ ftp	☒ hardware
☒ http	☒ http log
☒ icmp	☒ interface: eth0
☒ ip	☒ ip sockets
☒ line	☒ lpd
☒ memory	☒ processes
☒ query port	☒ rss
☒ sessions	☒ ssh
☒ syslog	☒ tcp
☒ telnet	☒ tftp
☒ tunnel	☒ udp
☒ vip	☒ xsr

Copyright © Lantronix, Inc. 2007-2010. All rights reserved.

2. Enter or modify the fields in [Table 13-4](#).

Table 13-4 XML Export Status Fields

Field	Description
Export to browser	Select this option to export the XML status record to a web browser.
Export to local file	Select this option to export the XML status record to a file on the device. If you select this option, enter a file name for the XML status record.
Lines to Export	Select the instances you want to export in the line, LPD, PPP, tunnel, and terminal groups.
Groups to Export	Check the configuration groups that are to be exported into the XML status record.

3. Click **Export**. The groups display if exporting to the browser. If exporting to the file system, the MatchPort AR requests a filename.

XML Import Configuration

To import a system configuration from an XML file, perform the following steps.

1. Click **XML > Import Configuration**. [Figure 13-7](#) shows the page that displays.

Figure 13-7 Import Configuration Web Page

Export Configuration Export Status **Import Configuration**

XML: Import Configuration

Import:

- ☐ Configuration from External file
- ☐ Configuration from Filesystem
- ☐ Line(s) from single line Settings on the Filesystem

Copyright © [Lantronix, Inc.](#) 2007-2010. All rights reserved.

2. Click one of the following radio buttons:
 - ◆ Configuration from External file. [See Import Configuration from External File on page 136.](#)
 - ◆ Configuration from Filesystem. [See Import Configuration from Filesystem on page 137.](#)
 - ◆ Line(s) from single line Settings on the Filesystem. [See Import Line\(s\) from Single Line Settings on the Filesystem on page 139.](#)

Import Configuration from External File

This selection shows a field for entering the path and file name of the entire external XCR file you want to import. You can also browse to select the XCR file.

To import a configuration file from an external file, perform the following steps.

1. Click **XML > Import Configuration > Configuration from External file**. [Figure 13-8](#) shows the page that displays.

Figure 13-8 Import Configuration from External File Web Page

Export Configuration Export Status **Import Configuration**

XML: Import Configuration

Import configuration from (entire) external XCR file:

Copyright © Lantronix, Inc. 2007-2010. All rights reserved.

2. Enter the path and file name of the external XCR file you want to import or browse to select the XCR file.
3. Click **Import**.

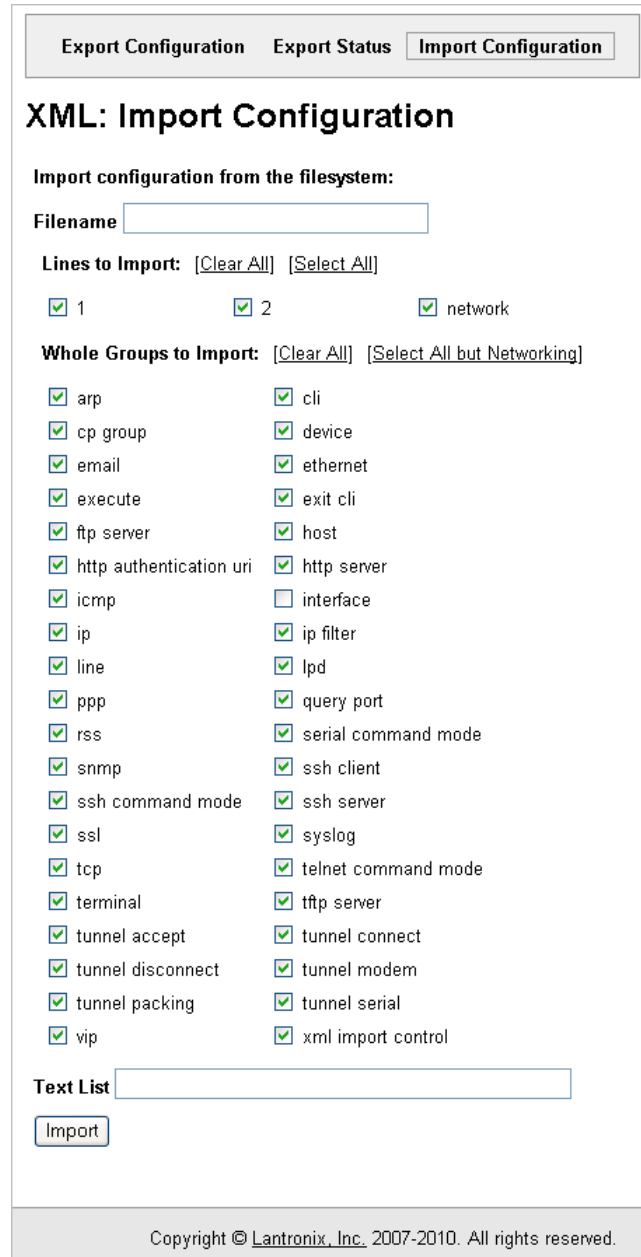
Import Configuration from Filesystem

This selection shows a page for entering the filesystem and your import requirements – groups, lines, and instances.

To import a configuration file from the Filesystem, perform the following steps.

1. Click **XML > Import Configuration > Configuration from Filesystem**. [Figure 13-9](#) shows the page that displays.

Figure 13-9 Import Configuration from Filesystem Web Page



2. Enter the fields shown in [Table 13-5](#).

Table 13-5 Import Configuration from Filesystem Fields

Field	Description
Filename	Enter the name of the file on the MatchPort AR (local to its filesystem) that contains XCR data.

Table 13-5 Import Configuration from Filesystem Fields (continued)

Field	Description
Lines to Import	Select the lines or network whose settings you want to import. Click the Select All link to select all the serial lines and the network lines. Click the Clear All link to clear all of the checkboxes. By default, all line instances are selected. Only the selected line instances will be imported in the line, LPD, PPP, tunnel, and terminal groups.
Whole Groups to Import	Select the configuration groups to import from the XML configuration record. This option imports all instances of each selected group unless it is one of the Lines to Import. Note: By default, all groups are checked except those pertaining to the network configuration; this is so that import will not break your network connectivity. You may check or uncheck any group to include or omit that group from import. To import all of the groups, click the Select All but Networking link to import all groups. To clear all the checkboxes, click the Clear All link.
Text List	Enter a string 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 specify the group name <g> only. Use this option for groups other than those affected by Lines to Import.

3. Click **Import**.

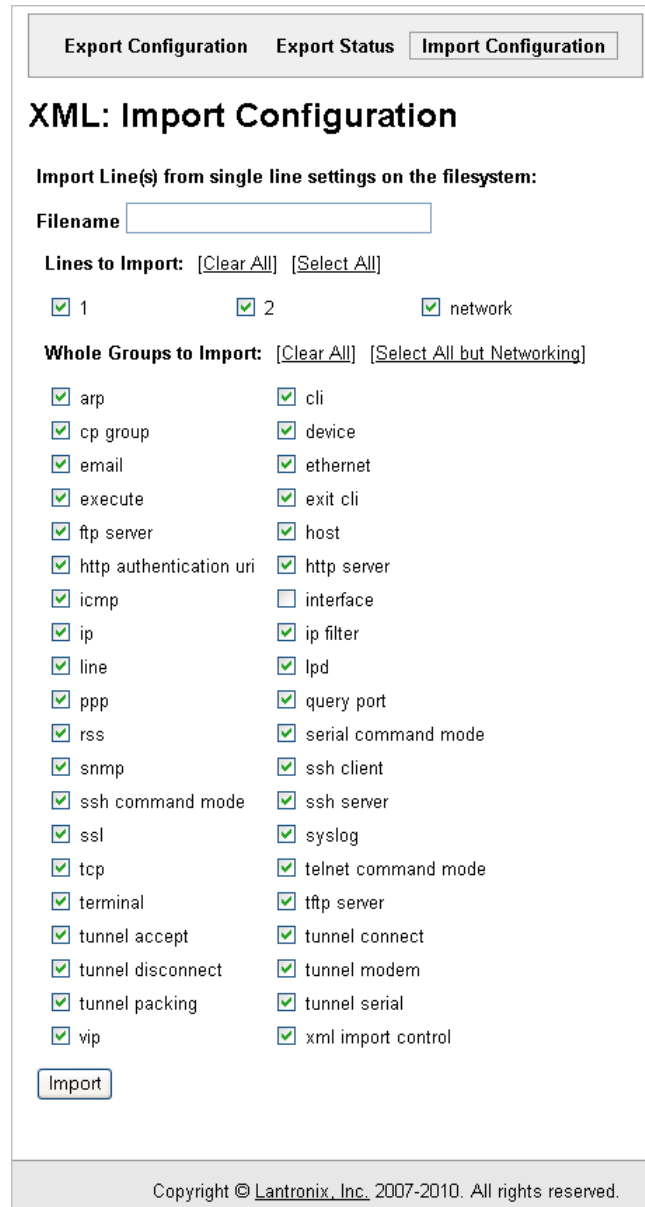
Import Line(s) from Single Line Settings on the Filesystem

This selection copies line settings from the single line instance in the input file to selected lines. The import file may only contain records from a single line instance; this is done by selecting a single line to export when exporting the file.

To import line settings on the Filesystem, perform the following steps.

1. Click **XML > Import Configuration > Line(s) from single line Settings on the Filesystem**. [Figure 13-10](#) shows the page that displays.

Figure 13-10 Import Lines from Single Line Settings on the Filesystem Web Page



2. Enter or modify the fields in [Table 13-6](#).

Table 13-6 Import Lines from Single Line Settings Fields

Field	Description
Filename	Provide the name of the file on the MatchPort AR (local to its file system) that contains XCR data.
Lines to Import	Select the line(s) whose settings you want to import. Click the Select All link to select all the serial lines and the network lines. Click the Clear All link clear all of the checkboxes. By default, all serial line instances are selected.

Table 13-6 Import Lines from Single Line Settings Fields (continued)

Field	Description
Whole Groups to Import	Select the configuration groups to import from the XML configuration record. Note: By default, all groups are checked except #those pertaining to the network configuration; this is so that import will not break your network connectivity. You may check or uncheck any group to include or omit that group from import. To import all of the groups, click the Select All but Networking link to import all groups. To clear all the checkboxes, click the Clear All link.

3. Click **Import**.

14: Branding the MatchPort AR

This chapter describes how to brand your MatchPort AR by using Web Manager and Command Line Interface (CLI). It contains the following sections:

- ◆ [Web Manager Customization](#)
- ◆ [Short and Long Name Customization](#)

Web Manager Customization

Customize the Web Manager appearance by modifying index.html and style.css. The style (fonts, colors, and spacing) of the Web Manager get controlled with style.css and the text and graphics are controlled with index.html.

The Web Manager files are hidden and are incorporated directly into the firmware image but may be overridden by placing the appropriate file in the appropriate directory on the file system.

To retrieve and overwrite Web Manager files, perform the following steps.

1. FTP to the MatchPort AR.
2. Make a directory (**mkdir**) and name it http/config.
3. Change to the directory (**cd**) that you created in Step 2 (http/config).
4. Get the file by using **get** <filename>.
5. Modify the file as required or create a new one with the same name.
6. Put the file by using **put** <filename>.
7. Type **quit**.

The overriding files display in the http/config directory. Restart any open browser to view the changes. If you want to return to the default files in the firmware image, delete the overriding files from the file system.

Short and Long Name Customization

You can customize the short and long names in Web Manager. The names display in the CLI show command and in the **System** web page in the Current Configuration table.. The short name is used for the show command. Both names display in the CLI Product Type field in the following example:

```
enable)# show
Product Information: MatchPort AR-YourCompanyName
Product Type: Lantronix MatchPort AR
```

In the Web Manager, the short and long names are shown in the **System** web page in the Current Configuration table.

To change the short and long names by using the Web Manager, perform the following steps.

1. Click **System** in the menu bar. [Figure 14-1](#) shows the page that displays.

Figure 14-1 System Branding Web Page

Name

Short Name:

Long Name:

Current Configuration

Firmware Version:	5.1.0.0R10
Short Name:	matchport_ar
Long Name:	Lantronix MatchPort AR

Copyright © [Lantronix, Inc.](#) 2007-2010. All rights reserved.

2. In the **Short Name** field, enter a short name up to 32 characters.
3. In the **Long Name** field, enter a long name up to 64 characters.
4. Click **Submit**.
5. Click **Reboot** to display the names.

15: Updating Firmware

Obtain the most up-to-date firmware and release notes for the MatchPort AR from the Lantronix Web site (www.lantronix.com/support/downloads/) or by using anonymous FTP (<ftp://ftp.lantronix.com/>). To upload new firmware, perform the following steps.

1. Click **System** in the Main Menu. [Figure 15-1](#) shows the page that displays.

Figure 15-1 System Web Page

The screenshot shows a web interface titled "System". It contains several sections: "Reboot Device" with a "Reboot" button; "Restore Factory Defaults" with a "Factory Defaults" button; "Upload New Firmware" with a file input field, a "Browse..." button, and an "Upload" button; "Name" with "Short Name:" and "Long Name:" labels and input fields, and a "Submit" button; and "Current Configuration" which is a table showing the current system settings.

Current Configuration	
Firmware Version:	5.1.0.0R7
Short Name:	EDS2100
Long Name:	Lantronix EDS2100

Copyright © Lantronix, Inc. 2007-2010. All rights reserved.

2. Click **Browse** in the **Upload New Firmware** section. The Choose File window displays.
3. Highlight the file and click Open.
4. Click **Upload** to install the firmware. The device automatically reboots on the installation of new firmware.

Alternatively, firmware can be updated by sending the file to the MatchPort AR over a FTP or TFTP connection.

A: Technical Support

If you are unable to resolve an issue by using the information in this user guide, please contact Technical Support at the following web site or phone numbers:

Technical Support US

Check our online knowledge base or send a question to Technical Support at www.lantronix.com/support.

Technical Support Europe, Middle East, Africa

Phone: +33 13 930 4172

Email: eu_techsupp@lantronix.com or eu_support@lantronix.com

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

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

- ◆ Your name, and your company name, address, and phone number
- ◆ Lantronix model number
- ◆ Lantronix serial number
- ◆ Firmware version (on the first screen shown when you Telnet to the device and type show)
- ◆ Description of the problem
- ◆ Status of the unit when the problem occurred (please try to include information on user and network activity at the time of the problem)
- ◆ Additionally, it may be useful to export and submit the XML Configuration and XML Status files

B: Binary to Hexadecimal Conversions

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

Use this chapter to learn to convert binary values to hexadecimal or to look up hexadecimal values in the tables of configuration options. The tables include:

- ◆ Command Mode (serial string sign-on message)
- ◆ AES Keys

Converting Binary to Hexadecimal

Following are two simple ways to convert binary numbers to hexadecimal notation.

Conversion Table

Hexadecimal digits have values ranging from 0 to F, which are represented as 0-9, A (for 10), B (for 11), etc. To convert a binary value (for example, 0100 1100) to a hexadecimal representation, treat the upper and lower four bits separately to produce a two-digit hexadecimal number (in this case, 4C).

Use the following table to convert values from binary to hexadecimal.

Table B-1 Conversion Values

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

Table B-1 Conversion Values (continued)

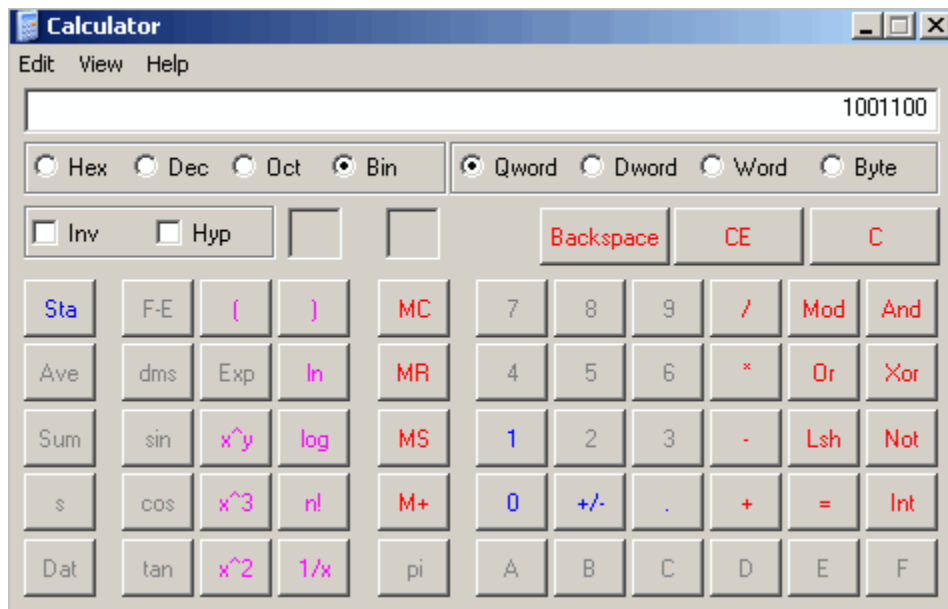
Decimal	Binary	Hex
14	1110	E
15	1111	F

Scientific Calculator

Another simple way to convert binary to hexadecimal is to use a scientific calculator, such as the one available on the Windows operating systems. For example:

1. On the Windows Start menu, click **Programs > Accessories > Calculator**.
2. On the View menu, select **Scientific**. The scientific calculator appears.
3. Click **Bin** (Binary) and type the number you want to convert.

Figure B-2 Scientific Calculator



4. Click **Hex**. The hexadecimal value appears.

Figure B-3 Hex Display



C: Compliance

Declaration of Conformity

According to ISO/IEC Guide 17050-1, 17050-2 and EN 45014

Manufacturer Name & Address

Lantronix, Inc.,
167 Technology, Irvine, CA 92618 USA

Product Name Model

MatchPort AR Embedded Device Server

Conforms to the following standards or other normative documents:

Radiated and conducted emissions

CFR Title 47 FCC Part 15, Subpart B and C
Industry Canada ICES-003 Issue 4 2004
VCCI V-3/2007.04
AS/NZS CISPR 22: 2006
EN55022: 1998 + A1: 2000 + A2: 2003
EN61000-3-2: 2000 + A2: 2005
EN61000-3-3: 1995 + A1: 2001 + A2: 2005

Immunity

EN55024: 1998 + A1: 2001 + A2: 2003

Direct & Indirect ESD

EN61000-4-2: 1995

RF Electromagnetic Field Immunity

EN61000-4-3: 2002

Electrical Fast Transient/Burst Immunity

EN61000-4-4: 2004

Surge Immunity

EN61000-4-5: 2006

RF Common Mode Conducted Susceptibility

EN61000-4-6: 1996

Power Frequency Magnetic Field Immunity

EN61000-4-8: 1994

Voltage Dips and Interrupts

EN61000-4-11: 2004

Safety

UL 60950-1
CAN/CSA-C22.2 No. 60950-1-03
EN 60950-1:2001, Low Voltage Directive (73/23/EEC)

RoHS Notice

All Lantronix products in the following families are China RoHS-compliant and free of the following hazardous substances and elements:

- ◆ Lead (Pb)
- ◆ Mercury (Hg)
- ◆ Cadmium (Cd)
- ◆ Hexavalent Chromium (Cr (VI))
- ◆ Polybrominated biphenyls (PBB)
- ◆ Polybrominated diphenyl ethers (PBDE)

Product Family Name	Toxic or hazardous Substances and Elements					
	Lead (Pb)	Mercury (Hg)	Cadmium (Cd)	Hexavalent Chromium (Cr (VI))	Polybrominated biphenyls (PBB)	Polybrominated diphenyl ethers (PBDE)
UDS1100 and 2100	0	0	0	0	0	0
EDS	0	0	0	0	0	0
MSS100	0	0	0	0	0	0
IntelliBox	0	0	0	0	0	0
XPress DR and XPress-DR+	0	0	0	0	0	0
SecureBox 1101 and 2101	0	0	0	0	0	0
WiBox	0	0	0	0	0	0
UBox	0	0	0	0	0	0
MatchPort	0	0	0	0	0	0
SLC	0	0	0	0	0	0
XPort	0	0	0	0	0	0
WiPort	0	0	0	0	0	0
SLB	0	0	0	0	0	0
SLP	0	0	0	0	0	0
SCS	0	0	0	0	0	0
SLS	0	0	0	0	0	0
DSC	0	0	0	0	0	0

0: Toxic or hazardous substance contained in all of the homogeneous materials for this part is below the limit requirement in SJ/T11363-2006.

x: Toxic or hazardous substance contained in at least one of the homogeneous materials used for this part is above the limit requirement in SJ/T11363-2006.

Manufacturer Contact

Lantronix Inc.

167 Technology, Irvine, CA 92618 USA

Phone: 949-453-3990

Fax: 949-450-7249

Index

A

- about this guide 12
 - additional documentation 13
 - chapter summaries 12
 - conventions 13
- advanced settings
 - CLI configuration 130
 - CLI statistics 130
 - command line interface 129
 - email configuration 128
 - email statistics 127
 - xml configuration 132
 - export status 134
 - import configuration 135
 - xml export configuration 132

B

- binary to hex conversion 146
 - conversion table 146
 - hex display 147
 - scientific calculator 147

C

- command line interface 17
- command line interface settings 129
- compliance
 - RoHS notice 149

D

- default server port numbers 19
- device control 17
- device details summary 21
- device management 18
- deviceinstaller
 - accessing the MatchPort AR 21
 - device details summary 21
 - using 21
- diagnostic toolset 18

E

- email configuration 128
- encrypt ion 18
- Enterprise-Grade Security 17

- ethernet address 19
- Europe, Middle East and Africa technical support 145
- Evolution OS™ 16

F

- Filesystem 26

H

- host configuration 62

L

- Lantronix discovery protocol 19
- line settings 32
 - command mode 35
 - configuration 33
 - statistics 32

M

- maintenance and diagnostics settings 106
 - diagnostics
 - buffer pools 123
 - DNS lookup 121
 - hardware 116
 - IP sockets 118
 - memory 122
 - MIB-II 117
 - ping 118
 - processes 123
 - traceroute 120
 - filesystem 106
 - browser 107
 - statistics 106
 - IP address filter 114
 - protocol stack 110
 - ARP 113
 - ICMP 112
 - IP 111
 - TCP 110
 - query port 115
 - system 125

N

- network settings
 - ethernet link 30

- interface configuration 29
- interface status 28

O

overview

- addresses and port numbers 19
- configurations methods 18
 - CLI 18
 - deviceinstaller 18
 - web manager 18
 - xml 19
- Evolution OS™ 16
- hardware address 19
- IP address 19
- port numbers 19
- product information label 19
- protocol support 16
- software features 16
 - CLI 17
 - enterprise-grade security 17
 - modem emulation 16
 - rss 17
 - snmp management 17
 - terminal server/device management 18
 - troubleshooting capabilities 18
 - vip access 17
 - web-based configuration and troubleshooting 17
 - xml-based architecture and device control 17

P

- port numbers 19

R

- rss 17

S

- secure com port redirector 18
- security
 - enterprise-grade 17
- security settings
 - SSH client known hosts 93
 - SSH client user configuration 94
 - SSH server authorized users 91
 - SSH server host keys 89
 - SSL certificates 97

- SSL certificates and private keys 98
- SSL cipher suites 96
- SSL configuration 99
- SSL rsa or dsa 97
- SSL utilities 98

services settings 70

- chap authentication 71
- dns status and cache 70
- ftp 75
- http 79
 - authentication 83
 - configuration 80
 - statistics 79
- lpd
 - 86
 - configuration 87
 - statistics 86
- ppp configuration 71
- rss 84
- snmp configuration 74
- syslog 78
- tftp 77

snmp management 17

SSH

- client known hosts 93
- protection level 17

SSL

- protection level 17

T

terminal

- server 18

terminal settings

- line terminal configuration 60
- network terminal configuration 59

troubleshooting capabilities 18

tunnel settings 37

- accept mode 44
- connect mode 46
- disconnect mode 54
- host list promotion 53
- modem emulation 55
 - command mode 55
- multiple hosts 51
- packing mode 40
- sequential host mode 51
- serial settings 39
- simultaneous host mode 51
- statistics 38

U

updating firmware 144
US technical support 145

V

VIP
 bootstrap file 102
 configurations 104
 configure tunnels for VIP 103
 enable VIP 103
 importing a bootstrap file 102
 statistics 103

W

web manager
 accessing 23
 components of typical web page 25
 configuration 23
 navigating 26
 navigation 26
 summary of web pages 26
web-based configuration 17

X

xml 19
xml configuration 132