<table>
<thead>
<tr>
<th>Date</th>
<th>Rev.</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>May 2009</td>
<td>C</td>
<td>Technical updates throughout; added RoHS notice.</td>
</tr>
<tr>
<td>May 2010</td>
<td>D</td>
<td>Updated for firmware release 5.1.0.0R10. Added VIP Access and Multiple Hosts in Connect Mode.</td>
</tr>
<tr>
<td>October 2013</td>
<td>E</td>
<td>Updated for firmware release 5.2.0.4.</td>
</tr>
</tbody>
</table>
# Table of Contents

**Intellectual Property** .................................................. 2
**Warranty** ..................................................................... 2
**Contacts** ...................................................................... 2
**Disclaimer** .................................................................... 2
**Revision History** .......................................................... 2
**List of Tables** ............................................................... 9
**List of Figures** ............................................................. 11

## 1: About This Guide

- Chapter and Appendix Summaries ........................................ 14
- Additional Documentation .................................................. 15

## 2: Introduction

- Key Features .................................................................... 16
- Applications ..................................................................... 17
- Protocol Support ............................................................. 17
- Evolution OS® Operating System ......................................... 17
- Additional Features .......................................................... 18
  - Modem Emulation .......................................................... 18
  - Web-Based Configuration and Troubleshooting .................. 18
  - Command-Line Interface (CLI) ........................................ 18
  - SNMP Management ...................................................... 18
  - XML-Based Architecture and Device Control .................... 18
  - Really Simple Syndication (RSS) ...................................... 18
  - Enterprise-Grade Security .............................................. 18
  - Terminal Server/Device Management ................................ 19
  - Troubleshooting Capabilities .......................................... 19
- Configuration Methods ...................................................... 20
- Addresses and Port Numbers .............................................. 20
  - Hardware Address ........................................................ 20
  - IP Address ..................................................................... 20
  - Port Numbers .............................................................. 20
- Product Information Label .................................................. 21

## 3: Using DeviceInstaller

- Accessing MatchPort AR Device Server Using DeviceInstaller ........................................ 22
- Device Details Summary .................................................. 22
4: Configuration Using Web Manager  
- Accessing Web Manager 
- Device Status Page 
- Web Manager Page Components 
- Navigating the Web Manager

5: Network Settings  
- Network 1 (eth0) Interface Status  
- Network 1 (eth0) Interface Configuration  
- Network 1 Ethernet Link

6: Line and Tunnel Settings  
- Line Settings  
  - Line Statistics 
  - Line Configuration 
  - Line Command Mode 
- Tunnel Settings  
  - Tunnel – Statistics 
  - Tunnel – Serial Settings 
  - Tunnel – Packing Mode 
  - Tunnel – Accept Mode 
  - Tunnel – Connect Mode 
  - Tunnel – Disconnect Mode 
  - Tunnel – Modem Emulation

7: Terminal and Host Settings  
- Terminal Settings  
  - Network Terminal Configuration 
  - Line Terminal Configuration 
- Host Configuration

8: Configurable Pin Manager  
- Overview 
- Default Groups 
- Custom Groups 
- CPM: CP (Configurable Pins)  
  - View CPs 
- CPM: Groups 
  - View Groups
## 9: Service Settings

<table>
<thead>
<tr>
<th>DNS Settings</th>
<th>66</th>
</tr>
</thead>
<tbody>
<tr>
<td>Point-to-Point (PPP) Settings</td>
<td>67</td>
</tr>
<tr>
<td>SNMP Settings</td>
<td>69</td>
</tr>
<tr>
<td>FTP Settings</td>
<td>71</td>
</tr>
<tr>
<td>TFTP Settings</td>
<td>72</td>
</tr>
<tr>
<td>Syslog Settings</td>
<td>73</td>
</tr>
<tr>
<td>HTTP Settings</td>
<td>74</td>
</tr>
<tr>
<td>HTTP Statistics</td>
<td>74</td>
</tr>
<tr>
<td>HTTP Configuration</td>
<td>75</td>
</tr>
<tr>
<td>HTTP Authentication</td>
<td>77</td>
</tr>
<tr>
<td>RSS Settings</td>
<td>79</td>
</tr>
<tr>
<td>LPD Settings</td>
<td>80</td>
</tr>
<tr>
<td>LPD Statistics</td>
<td>80</td>
</tr>
<tr>
<td>LPD Configuration</td>
<td>81</td>
</tr>
</tbody>
</table>

## 10: Security Settings

<table>
<thead>
<tr>
<th>SSH Settings</th>
<th>83</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSH Server Host Keys</td>
<td>84</td>
</tr>
<tr>
<td>SSH Server Authorized Users</td>
<td>88</td>
</tr>
<tr>
<td>SSH Client Known Hosts</td>
<td>90</td>
</tr>
<tr>
<td>SSH Client Users</td>
<td>91</td>
</tr>
<tr>
<td>SSL Settings</td>
<td>93</td>
</tr>
<tr>
<td>SSL Cipher Suites</td>
<td>93</td>
</tr>
<tr>
<td>SSL Certificates</td>
<td>94</td>
</tr>
<tr>
<td>SSL RSA or DSA</td>
<td>94</td>
</tr>
<tr>
<td>SSL Certificates and Private Keys</td>
<td>94</td>
</tr>
<tr>
<td>SSL Utilities</td>
<td>95</td>
</tr>
<tr>
<td>SSL Configuration</td>
<td>96</td>
</tr>
</tbody>
</table>

## 11: Modbus

| CP Control via Modbus | 99 |
| Serial Transmission Mode | 101 |
| Modbus Statistics | 102 |
| Modbus Configuration | 103 |

## 12: Maintenance and Diagnostics Settings

| Filesystem Settings | 104 |
| Filesystem Statistics | 104 |
| Filesystem Browser | 105 |
| Protocol Stack Settings | 107 |
| TCP Settings | 107 |
IP Settings 108
ICMP Settings 109
ARP Settings 110
SMTP Settings 111
IP Address Filter 112
Query Port 113
Diagnostics 114
Hardware 114
MIB-II Statistics 115
IP Sockets 116
Ping 116
Traceroute 117
Log 118
Memory 119
Buffer Pools 120
Processes 121
System Settings 122

13: Advanced Settings 124
Email Settings 124
Email Statistics 124
Email Configuration 125
Command Line Interface Settings 127
CLI Statistics 127
CLI Configuration 127
XML Settings 129
XML: Export Configuration 130
XML: Export Status 131
XML: Import Configuration 132

14: Security in Detail 137
Public Key Infrastructure 137
TLS (SSL) 137
Digital Certificates 137
Trusted Authorities 137
Obtaining Certificates 138
Self-Signed Certificates 138
Certificate Formats 138
OpenSSL 138
List of Tables

Table 3-1 Device Details Summary ................................................................. 22
Table 4-4 Summary of Web Manager Pages .................................................. 27
Table 5-3 Network 1 (eth0) Interface Configuration .................................. 30
Table 5-5 Network 1 Ethernet Link ............................................................... 32
Table 6-3 Line Configuration ...................................................................... 35
Table 6-5 Line Command Mode ................................................................. 36
Table 6-8 Tunnel - Serial Settings .............................................................. 40
Table 6-12 Tunnel Packing Mode ............................................................... 43
Table 6-14 Tunnel Accept Mode ............................................................... 44
Table 6-16 Tunnel Connect Mode ............................................................. 48
Table 6-19 Tunnel Disconnect Mode ......................................................... 51
Table 6-20 Modem Emulation Commands and Descriptions ...................... 52
Table 6-22 Tunnel Modem Emulation ......................................................... 54
Table 7-2 Terminal on Network Configuration ........................................... 56
Table 7-4 Terminal on Line 1 Configuration ............................................... 57
Table 7-6 Host Configuration ................................................................. 58
Table 8-2 CPM CPs Current Configuration ................................................. 61
Table 8-3 CPM CPs Status ............................................................... 61
Table 8-5 CPM Groups Current Configuration ............................................. 62
Table 8-7 Group Status ................................................................. 63
Table 9-3 PPP Configuration ................................................................. 68
Table 9-5 SNMP ................................................................. 70
Table 9-7 FTP Settings ................................................................. 71
Table 9-9 TFTP Server ................................................................. 72
Table 9-11 Syslog ................................................................. 73
Table 9-14 HTTP Configuration ............................................................. 75
Table 9-16 HTTP Authentication ............................................................. 77
Table 9-18 RSS ................................................................. 79
Table 9-21 LPD Configuration ............................................................... 81
Table 10-2 SSH Server Host Keys Settings - Upload Keys Method ............. 85
Table 10-4 SSH Server Host Keys Settings - Upload Keys Method ............. 86
Table 10-6 SSH Server Host Keys Settings - Create New Keys Method ......... 87
Table 10-8 SSH Server Authorized User Settings ..................................... 89
Table 10-10 SSH Client Known Hosts ....................................................... 90
Table 10-12 SSH Client Users ............................................................... 92
List of Figures

Figure 2-1 Sample Hardware Address _______________________________________________ 20
Figure 2-2 Product Label __________________________________________________________ 21
Figure 4-1 Prompt for User Name and Password ______________________________________ 24
Figure 4-2 Web Manager Home Page _______________________________________________ 25
Figure 4-3 Components of the Web Manager Page ____________________________________ 26
Figure 5-1 Network 1 (eth0) Interface Status _________________________________________ 29
Figure 5-2 Network 1 (eth0) Interface Configuration _________________________________ 30
Figure 5-4 Network 1 Ethernet Link ________________________________________________ 32
Figure 6-1 Line 1 Statistics ________________________________________________________ 33
Figure 6-2 Line 1 Configuration ___________________________________________________ 34
Figure 6-4 Line 1 Command Mode __________________________________________________ 36
Figure 6-6 Tunnel 1 Statistics _____________________________________________________ 39
Figure 6-7 Tunnel 1 Serial Settings _______________________________________________ 40
Figure 6-9 Tunnel 1 Packing Mode (Mode = Disable) ___________________________________ 41
Figure 6-10 Tunnel 1 Packing Mode (Mode = Timeout) ________________________________ 42
Figure 6-11 Tunnel 1 Packing Mode (Mode = Send Character) ___________________________ 42
Figure 6-13 Tunnel 1 Accept Mode ________________________________________________ 44
Figure 6-15 Tunnel 1 - Connect ____________________________________________________ 47
Figure 6-17 Host 1, Host 2, Host 3 Exchanged __________________________________________ 50
Figure 6-18 Tunnel 1 Disconnect Mode ______________________________________________ 51
Figure 6-21 Tunnel 1 Modem Emulation _____________________________________________ 53
Figure 7-1 Terminal on Network Configuration ________________________________________ 55
Figure 7-3 Terminal on Line Configuration ___________________________________________ 56
Figure 7-5 Host Configuration _____________________________________________________ 58
Figure 8-1 CPM: CPs ______________________________________________________________ 60
Figure 8-4 CPM: Groups __________________________________________________________ 62
Figure 8-6 CPM: Group Status _____________________________________________________ 63
Figure 9-1 DNS Settings __________________________________________________________ 66
Figure 9-2 PPP Configuration Settings ______________________________________________ 68
Figure 9-4 SNMP Configuration ____________________________________________________ 69
Figure 9-6 FTP Configuration _____________________________________________________ 71
Figure 9-8 TFTP Configuration ____________________________________________________ 72
Figure 9-10 Syslog ______________________________________________________________ 73
Figure 9-12 HTTP Statistics ______________________________________________________ 74
Figure 9-13 HTTP Configuration __________________________________________________ 75
Figure 9-15 HTTP Authentication ................................................................. 77
Figure 9-17 RSS ....................................................................................... 79
Figure 9-19 LPD Statistics .............................................................. 80
Figure 9-20 LPD Configuration ............................................ 81
Figure 10-1 SSH Server: Host Keys (Upload Keys) ............... 84
Figure 10-3 SSH Server: Host Keys (Upload Keys) ............... 86
Figure 10-5 SSH Server: Host Keys (Create New Keys) .......... 87
Figure 10-7 SSH Server: Authorized Users ..................... 89
Figure 10-9 SSH Client: Known Hosts ........................................ 90
Figure 10-11 SSH Client: Users .................................................. 91
Figure 10-14 SSL ........................................................................... 96
Figure 11-5 Modbus Statistics ............................................. 102
Figure 11-6 Modbus Configuration .................................... 103
Figure 12-1 Filesystem Statistics ........................................ 104
Figure 12-2 Filesystem Browser ........................................ 105
Figure 12-4 TCP Protocol .......................................................... 107
Figure 12-6 IP Protocol ............................................................... 108
Figure 12-8 ICMP Protocol ......................................................... 109
Figure 12-10 ARP Protocol Page ...................................... 110
Figure 12-12 SMTP ................................................................. 111
Figure 12-14 IP Address Filter Configuration ............. 112
Figure 12-16 Query Port Configuration ....................... 113
Figure 12-17 Diagnostics: Hardware ............................... 114
Figure 12-18 MIB-II Network Statistics .................... 115
Figure 12-19 IP Sockets .......................................................... 116
Figure 12-20 Diagnostics: Ping ............................................. 117
Figure 12-22 Diagnostics: Traceroute ............................... 118
Figure 12-24 Diagnostics: Log ............................................... 118
Figure 12-25 Diagnostics: Log (Filesystem) ..................... 119
Figure 12-26 Diagnostics: Log (Line 1) ............................... 119
Figure 12-27 Diagnostics: Memory ................................. 120
Figure 12-28 Diagnostics: Buffer Pools ..................... 120
Figure 12-29 Diagnostics: Processes ............................... 121
Figure 12-30 System ................................................................. 122
Figure 13-1 Email Statistics ...................................................... 124
Figure 13-2 Email Configuration ..................................... 125
Figure 13-4 CLI Statistics .......................................................... 127
Figure 13-5 CLI Configuration ............................................. 128
1: About This Guide

This guide provides the information needed to configure, use, and update the MatchPort® AR embedded device server. It is intended for software developers and system integrators who are embedding the embedded device server in their designs.

Chapter and Appendix Summaries

A summary of each chapter is provided below.

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter 2: Introduction</td>
<td>Main features of the product and the protocols it supports. Includes technical specifications.</td>
</tr>
<tr>
<td>Chapter 3: Using DeviceInstaller</td>
<td>Instructions for viewing the current configuration using DeviceInstaller.</td>
</tr>
<tr>
<td>Chapter 4: Configuration Using Web Manager</td>
<td>Instructions for accessing Web Manager and using it to configure settings for the device.</td>
</tr>
<tr>
<td>Chapter 5: Network Settings</td>
<td>Instructions for using the web interface to configure Ethernet settings.</td>
</tr>
<tr>
<td>Chapter 6: Line and Tunnel Settings</td>
<td>Instructions for using the web interface to configure line and tunnel settings.</td>
</tr>
<tr>
<td>Chapter 7: Terminal and Host Settings</td>
<td>Instructions for using the web interface to configure terminal and host settings.</td>
</tr>
<tr>
<td>Chapter 8: Configurable Pin Manager</td>
<td>Information about the Configurable Pin Manager (CPM) and how to set the configurable pins to work with a device.</td>
</tr>
<tr>
<td>Chapter 9: Service Settings</td>
<td>Instructions for using the web interface to configure settings for DNS, SNMP, FTP, and other services.</td>
</tr>
<tr>
<td>Chapter 10: Security Settings</td>
<td>Instructions for using the web interface to configure SSH and SSL security settings.</td>
</tr>
<tr>
<td>Chapter 11: Modbus</td>
<td>Instructions for using the web interface to configure Modbus.</td>
</tr>
<tr>
<td>Chapter 12: Maintenance and Diagnostics Settings</td>
<td>Instructions for using the web interface to maintain the device, view statistics, files, and logs, and diagnose problems.</td>
</tr>
<tr>
<td>Chapter 13: Advanced Settings</td>
<td>Instructions for using the web interface to configure email, CLI, and XML settings.</td>
</tr>
<tr>
<td>Chapter 14: Security in Detail</td>
<td>Provides additional information on security settings available.</td>
</tr>
<tr>
<td>Chapter 15: Branding the MatchPort AR Unit</td>
<td>Instructions for customizing the device.</td>
</tr>
<tr>
<td>Chapter 16: Updating Firmware</td>
<td>Instructions for obtaining the latest firmware and updating the device.</td>
</tr>
<tr>
<td>Appendix B: Compliance</td>
<td>Lantronix compliance information.</td>
</tr>
<tr>
<td>Appendix C: Binary to Hexadecimal Conversions</td>
<td>Instructions for converting binary values to hexadecimals.</td>
</tr>
</tbody>
</table>
Additional Documentation

Visit the Lantronix web site at [www.lantronix.com/support/documentation](http://www.lantronix.com/support/documentation) for the latest documentation and the following additional documentation.

<table>
<thead>
<tr>
<th>Document</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MatchPort AR Embedded Device Server Command Reference</td>
<td>Information about the MatchPort AR hardware along with directions on integrating the device server into your product.</td>
</tr>
<tr>
<td>MatchPort AR Embedded Device Server Integration Guide</td>
<td>Instructions for accessing the 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.</td>
</tr>
<tr>
<td>MatchPort Embedded Device Server Demonstration Kit Quick Start Guide</td>
<td>Information about the device hardware installation and initial configuration of your device.</td>
</tr>
<tr>
<td>DeviceInstaller Online Help</td>
<td>Instructions for using the Lantronix Windows-based utility to locate the device and to view its current settings.</td>
</tr>
<tr>
<td>Com Port Redirector Quick Start and Online Help</td>
<td>Instructions for using the Lantronix Windows-based utility to create virtual com ports.</td>
</tr>
<tr>
<td>Secure Com Port Redirector User Guide</td>
<td>Instructions for using the Lantronix Windows-based utility to create secure virtual com ports.</td>
</tr>
</tbody>
</table>
2: Introduction

This chapter introduces the Lantronix MatchPort AR embedded device server. It provides an overview of the products, lists their key features, and describes the applications for which they are suited.

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 Features
- Applications
- Protocol Support
- Evolution OS® Operating System
- Additional Features
- Configuration Methods
- Addresses and Port Numbers
- Product Information Label

Key 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 embedded device server connects serial devices such as those listed below to Ethernet network 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 embedded device server contains a full-featured TCP/IP stack. Supported protocols include:

- ARP, IP, UDP, TCP, ICMP, BOOTP, DHCP, AutoIP, 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® Operating System

The MatchPort AR embedded device server incorporates the Lantronix Evolution OS operating system. Key features of the Evolution OS operating system 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
Additional Features

Modem Emulation
In modem emulation mode, the MatchPort AR device server 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 embedded device server enables you to configure, manage, and troubleshoot through a browser-based interface accessible anytime from anywhere. All configuration and troubleshooting options are launched from a 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 embedded device server with Evolution OS uses industry-standard tools for configuration, communication, and control. For example, 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.

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 device servers.

XML-Based Architecture and Device Control
XML is a fundamental building block for the future growth of M2M networks. The MatchPort AR embedded device server 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 device server 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 then reads (polls) the feed. 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 embedded device server 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.

With built-in SSH and SSL, secure communications can be established between the serial ports and the remote end device or application. 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 are able to do the following:

- 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 device server 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 embedded device server cannot be used to bring down other devices on the network.

You can use the MatchPort AR device server 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 embedded device server 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 menu system on the MatchPort device, connections to the console ports of the attached devices as well as network hosts, such as Unix servers or another MatchPort unit, can easily be picked from a user-defined menu. This allows console ports across multiple devices to be accessed from one MatchPort.

**Troubleshooting Capabilities**

The MatchPort AR embedded device server 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 device server, including CPU utilization and total stack space available.
Configuration Methods

After installation, the MatchPort AR embedded device server 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 using a Graphical User Interface (GUI) on a PC attached to a network. See Chapter 3: Using DeviceInstaller.

**Web Manager:** Through a web browser, configure the MatchPort AR settings using the Lantronix Web Manager. See Configuration Using Web Manager (on page 24).

**Command Mode:** There are two methods for accessing Command Mode (CLI): making a Telnet connection or connecting a terminal (or a PC running a terminal emulation program) to the unit’s serial port. (See the MatchPort AR Embedded Device Server Command Reference for instructions and available commands.)

**XML:** The MatchPort AR embedded device server 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. (See the MatchPort AR Embedded Device Server Command Reference for instructions and 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.

![Sample Hardware Address](image)

**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 embedded device server:

- 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

**Note:** Multi-port products include one or more additional supported ports and tunnels with default sequential numbering. For instance: TCP/UDP Port 10002: Tunnel 2, TCP/UDP Port 10003: Tunnel 3, etc.

**Product Information Label**

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

- Part Number
- Bar Code
- Revision
- Hardware Address (MAC Address or Serial Number)

![Figure 2-2 Product Label](image)
3: **Using DeviceInstaller**

This chapter covers the steps for locating a device and viewing its properties and details. The Lantronix DeviceInstaller™ application 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.html](http://www.lantronix.com/support/downloads.html). For instructions on using DeviceInstaller to configure the IP address, 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 Device Server Using DeviceInstaller

*Note:* Make note of the MAC address. It is needed to locate the MatchPort AR embedded device server using DeviceInstaller.

1. Click **Start > All Programs > Lantronix > DeviceInstaller > DeviceInstaller**.
   
   When DeviceInstaller starts, it will perform a network device search.

2. Click **Search** to perform additional searches, as desired.

3. Expand the MatchPort folder by clicking the + symbol next to the MatchPort folder icon. The list of available Lantronix MatchPort devices appears.

4. Select the MatchPort AR unit by expanding its entry and clicking on its hardware (MAC) or IP address to view its configuration.

5. On the right page, click the **Device Details** tab. The current MatchPort AR configuration appears. This is only a subset of the full configuration; the complete configuration may be accessed via Web Manager, CLI, or XML.

### Device Details Summary

*Note:* The settings are Display Only in this table unless otherwise noted.

<table>
<thead>
<tr>
<th>Current Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name identifying the MatchPort AR embedded device server.</td>
</tr>
<tr>
<td>DHCP Device Name</td>
<td>Shows the name associated with the current IP address, if the IP address was obtained dynamically.</td>
</tr>
<tr>
<td>Group</td>
<td>Configurable field. Enter a group to categorize the MatchPort AR embedded device server. 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.</td>
</tr>
<tr>
<td>Current Settings (continued)</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Comments</td>
<td>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.</td>
</tr>
<tr>
<td>Device Family</td>
<td>Shows the MatchPort AR device family type as “MatchPort.”</td>
</tr>
<tr>
<td>Short Name</td>
<td>Shows “matchport_ar” by default.</td>
</tr>
<tr>
<td>Long Name</td>
<td>Shows “MatchPort AR” by default.</td>
</tr>
<tr>
<td>Type</td>
<td>Shows the specific device type, such as “MatchPort AR”.</td>
</tr>
<tr>
<td>ID</td>
<td>Shows the MatchPort AR ID embedded within the unit.</td>
</tr>
<tr>
<td>Hardware Address</td>
<td>Shows the MatchPort AR hardware (MAC) address.</td>
</tr>
<tr>
<td>Firmware Version</td>
<td>Shows the firmware currently installed on the MatchPort AR.</td>
</tr>
<tr>
<td>Extended Firmware Version</td>
<td>Provides additional information on the firmware version.</td>
</tr>
<tr>
<td>Online Status</td>
<td>Shows the MatchPort AR status as Online, Offline, Unreachable (the MatchPort AR embedded device server is on a different subnet), or Busy (the MatchPort AR is currently performing a task).</td>
</tr>
<tr>
<td>IP Address</td>
<td>Shows the MatchPort AR current IP address. To change the IP address, click the Assign IP button on the DeviceInstaller menu bar.</td>
</tr>
</tbody>
</table>
| IP Address was Obtained     | Displays “Dynamically” if the MatchPort AR embedded device server automatically received an IP address (e.g., from DHCP). Displays “Static” if the IP address was configured manually. If the IP address was assigned dynamically, the following fields appear:  
  ◆ Obtain via DHCP with value of True or False.  
  ◆ Obtain via BOOTP with value of True or False. |
| Subnet Mask                 | Shows the subnet mask specifying the network segment on which the MatchPort AR embedded device server 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 unit. |
| Supports Configurable Pins  | Shows , indicating configurable pins are available on the MatchPort AR embedded device server. |
| Supports Email Triggers     | Shows True, indicating email triggers are available on the MatchPort AR unit. |
| Telnet Supported            | Indicates whether Telnet is enabled on this MatchPort AR embedded device server. |
| Telnet Port                 | Shows the MatchPort AR port for Telnet sessions. |
| Web Port                    | Shows the MatchPort AR port for Web Manager configuration. |
| Firmware Upgradable         | Shows True, indicating the MatchPort AR firmware is upgradable as newer versions become available. |
4: **Configuration Using Web Manager**

This chapter describes how to configure the MatchPort AR embedded device server using Web Manager, the Lantronix browser-based configuration tool. The unit’s 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 Page Components**
- **Navigating the Web Manager**
- **Summary of Web Manager Pages**

**Accessing Web Manager**

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

To access 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, Chrome 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 (see the Embedded Device Server 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 4-2 displays configuration, network settings, line settings, tunneling settings, and product information.

*Note:* The Logout button is available on any web page. Logging out of the web page would force re-authentication to take place the next time the web page is accessed.
Device Status Page

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

Figure 4-2  Web Manager Home Page

<table>
<thead>
<tr>
<th>Status</th>
<th>Device Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>CLI</td>
<td>Product Information</td>
</tr>
<tr>
<td>CPM</td>
<td>Product Type: Lantronix MatchPort AR</td>
</tr>
<tr>
<td>Diagnostics</td>
<td>Firmware Version: 5.2.0.4R1</td>
</tr>
<tr>
<td>DNS</td>
<td>Build Date: Aug 20 2013 (17:14:17)</td>
</tr>
<tr>
<td>Email</td>
<td>Serial Number: 076215547368/M2Z</td>
</tr>
<tr>
<td>Filesystem</td>
<td>Uptime: 8 days 09:33:01</td>
</tr>
<tr>
<td>FTP</td>
<td>Permanent Config: Saved</td>
</tr>
<tr>
<td>Host</td>
<td>Network Settings</td>
</tr>
<tr>
<td>HTTP</td>
<td>Interface: eth0</td>
</tr>
<tr>
<td>IP Address Filter</td>
<td>Link: Auto 10/100 Mbps Auto Half/Full (100 Mbps Full)</td>
</tr>
<tr>
<td>Line</td>
<td>MAC Address: 00:20:4a:a7:06:4b</td>
</tr>
<tr>
<td>LPD</td>
<td>Hostname: &lt;none&gt;</td>
</tr>
<tr>
<td>Modbus</td>
<td>IP Address: 172.19.223.100/16</td>
</tr>
<tr>
<td>Network</td>
<td>Default Gateway: 172.19.0.1</td>
</tr>
<tr>
<td>PPP</td>
<td>Domain: &lt;none&gt;</td>
</tr>
<tr>
<td>Protocol Stack</td>
<td>Primary DNS: 172.19.1.1</td>
</tr>
<tr>
<td>Query Port</td>
<td>Secondary DNS: 172.19.1.2</td>
</tr>
<tr>
<td>RSS</td>
<td>MTU: 1500</td>
</tr>
<tr>
<td>SNMP</td>
<td>VIP Conduit: Disabled</td>
</tr>
<tr>
<td>SSH</td>
<td>Line Settings</td>
</tr>
<tr>
<td>SSL</td>
<td>Line 1: RS232, 9600, None, 8, 1, None [CLI]</td>
</tr>
<tr>
<td>SSL</td>
<td>Line 2: RS232, 9600, None, 8, 1, None</td>
</tr>
<tr>
<td>Syng</td>
<td>Tunneling Connect Mode Accept Mode</td>
</tr>
<tr>
<td>System</td>
<td>Tunnel 1: Disabled Waiting</td>
</tr>
<tr>
<td>Terminal</td>
<td>Tunnel 2: Disabled Waiting</td>
</tr>
<tr>
<td>TFTP</td>
<td></td>
</tr>
<tr>
<td>Tunnel</td>
<td></td>
</tr>
<tr>
<td>VIP</td>
<td></td>
</tr>
<tr>
<td>XML</td>
<td></td>
</tr>
</tbody>
</table>

Copyright © Lantronix, Inc. 2007-2012. All rights reserved.
Web Manager Page Components

The layout of a typical Web Manager page is below.

![Figure 4-3 Components of the Web Manager Page](image)

The menu bar always appears at the left side of the page, regardless of the page shown. The menu bar lists the names of the pages available in the Web Manager. To bring up a page, click it in the menu bar.

The main area of the page has these additional sections:

- At the very top, many pages, such as the one in the example above, enable you to link to sub pages. On some pages, you must also select the item you are configuring, such as a line or a tunnel.

---

MatchPort® AR Embedded Device Server User Guide
In the middle of many pages, you can select or enter new configuration settings. Some pages show status or statistics in this area rather than allow you to enter settings.

At the bottom of most pages, the current configuration is displayed. In some cases, you can reset or clear a setting.

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

A Logout link is available at the upper right corner of every web page. In Chrome or Safari, it is necessary to close out of the browser to logout. If necessary, reopen the browser to log back in.

The footer appears at the very bottom of the page. It contains copyright information and 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>
<thead>
<tr>
<th>Web Manager Page</th>
<th>Description</th>
<th>See Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Shows product information and network, line, and tunneling settings.</td>
<td>33</td>
</tr>
<tr>
<td>CLI</td>
<td>Shows Command Line Interface (CLI) statistics and lets you change the current CLI configuration settings.</td>
<td>127</td>
</tr>
<tr>
<td>CPM</td>
<td>Shows information about the Configurable Pins Manager (CPM) and how to set the configurable pins and pin groups to work with a device.</td>
<td>59</td>
</tr>
<tr>
<td>CPU Power Management</td>
<td>Allows you to configure CPU power management, specifically the power management of the cpu, the on-chip peripherals and the extended memory.</td>
<td>136</td>
</tr>
<tr>
<td>Diagnostics</td>
<td>Lets you perform various diagnostic procedures.</td>
<td>114</td>
</tr>
<tr>
<td>DNS</td>
<td>Shows the current configuration of the DNS subsystem and the DNS cache.</td>
<td>66</td>
</tr>
<tr>
<td>Email</td>
<td>Shows email statistics and lets you clear the email log, configure email settings, and send an email.</td>
<td>124</td>
</tr>
<tr>
<td>Filesystem</td>
<td>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.</td>
<td>104</td>
</tr>
<tr>
<td>FTP</td>
<td>Shows statistics and lets you change the current configuration for the File Transfer Protocol (FTP) server.</td>
<td>71</td>
</tr>
<tr>
<td>Host</td>
<td>Lets you view and change settings for a host on the network.</td>
<td>57</td>
</tr>
<tr>
<td>HTTP</td>
<td>Shows HyperText Transfer Protocol (HTTP) statistics and lets you change the current configuration and authentication settings.</td>
<td>74</td>
</tr>
<tr>
<td>Web Manager Page (continued)</td>
<td>Description</td>
<td>See Page</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-------------</td>
<td>----------</td>
</tr>
<tr>
<td>IP Address Filter</td>
<td>Lets you specify all the IP addresses and subnets that are allowed to send data to this device.</td>
<td>112</td>
</tr>
<tr>
<td>Line</td>
<td>Shows statistics and lets you change the current configuration and Command mode settings of a serial line.</td>
<td>33</td>
</tr>
<tr>
<td>LPD</td>
<td>Shows LPD (Line Printer Daemon) Queue statistics and lets you configure the LPD and print a test page.</td>
<td>80</td>
</tr>
<tr>
<td>Modbus</td>
<td>Shows the current connection status of the Modbus servers listening on the TCP ports and lets you configure the Modbus settings.</td>
<td>99</td>
</tr>
<tr>
<td>Network</td>
<td>Shows status and lets you configure the network interface.</td>
<td>29</td>
</tr>
<tr>
<td>Protocol Stack</td>
<td>Lets you perform lower level network stack-specific activities.</td>
<td>107</td>
</tr>
<tr>
<td>Query Port</td>
<td>Lets you change configuration settings for the query port.</td>
<td>113</td>
</tr>
<tr>
<td>RSS</td>
<td>Lets you change current Really Simple Syndication (RSS) settings.</td>
<td>79</td>
</tr>
<tr>
<td>SNMP</td>
<td>Lets you change the current Simple Network Management Protocol (SNMP) configuration settings.</td>
<td>69</td>
</tr>
<tr>
<td>SSH</td>
<td>Lets you change the configuration settings for SSH server host keys, SSH server authorized users, SSH client known hosts, and SSH client users.</td>
<td>83</td>
</tr>
<tr>
<td>SSL</td>
<td>Lets you upload an existing certificate or create a new self-signed certificate.</td>
<td>93</td>
</tr>
<tr>
<td>Syslog</td>
<td>Lets you specify the severity of events to log and the server and ports to which the syslog should be sent.</td>
<td>73</td>
</tr>
<tr>
<td>System</td>
<td>Lets you reboot device, restore factory defaults, upload new firmware, and change the device long and short names.</td>
<td>122</td>
</tr>
<tr>
<td>Terminal</td>
<td>Lets you change current settings for a terminal.</td>
<td>55</td>
</tr>
<tr>
<td>TFTP</td>
<td>Shows statistics and lets you change the current configuration for the Trivial File Transfer Protocol (TFTP) server.</td>
<td>72</td>
</tr>
<tr>
<td>Tunnel</td>
<td>Lets you change the current configuration settings for a tunnel.</td>
<td>37</td>
</tr>
<tr>
<td>XML</td>
<td>Lets you export XML configuration and status records, and import XML configuration records.</td>
<td>129</td>
</tr>
</tbody>
</table>
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 Ethernet network interface and link.

This chapter contains the following sections:

- **Network 1 (eth0) Interface Status**
- **Network 1 (eth0) Interface Configuration**
- **Network 1 Ethernet Link**

**Network 1 (eth0) Interface Status**

This page shows the status of the Ethernet network interface.

*To view the network interface status:*

1. Click **Network** on the menu then click **Network 1 > Interface > Status** at the top of the page. The Network 1 (eth0) Interface Status page appears.

![Figure 5-1 Network 1 (eth0) Interface Status](image)

**Network 1 (eth0) Interface Status**

<table>
<thead>
<tr>
<th>Current</th>
<th>After Reboot</th>
</tr>
</thead>
<tbody>
<tr>
<td>BOOTP Client:</td>
<td>Off</td>
</tr>
<tr>
<td>DHCP Client:</td>
<td>Off</td>
</tr>
<tr>
<td>IP Address:</td>
<td>172.19.229.100</td>
</tr>
<tr>
<td>Network Mask:</td>
<td>255.255.0.0</td>
</tr>
<tr>
<td>Default Gateway:</td>
<td>172.19.0.1</td>
</tr>
<tr>
<td>Hostname:</td>
<td>&lt;None&gt;</td>
</tr>
<tr>
<td>Domain:</td>
<td>&lt;None&gt;</td>
</tr>
<tr>
<td>DNS Suffix Search List:</td>
<td>&lt;None&gt;</td>
</tr>
<tr>
<td>DHCP Client ID:</td>
<td>&lt;None&gt;</td>
</tr>
<tr>
<td>MTU:</td>
<td>1500</td>
</tr>
</tbody>
</table>
**Network 1 (eth0) Interface Configuration**

This page shows the configuration settings for the Ethernet connection and lets you change these settings.

*To view and configure network interface settings:*

1. Click **Network** on the menu bar and then **Network 1 > Interface > Configuration** at the top of the page. The Network 1 (eth0) Interface Configuration page appears.

2. Enter or modify the following settings:

   **Table 5-3  Network 1 (eth0) Interface Configuration**

<table>
<thead>
<tr>
<th>Network 1 Interface Configuration Settings</th>
<th>Description</th>
</tr>
</thead>
</table>
| BOOTP Client                              | Select On or Off. At boot up, the device 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. |

[Figure 5-2  Network 1 (eth0) Interface Configuration]
### Network 1 Interface Configuration Settings (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DHCP Client</strong></td>
<td>Select <strong>On</strong> or <strong>Off</strong>. At boot up, the device will attempt to lease an IP address from a DHCP server and maintain the lease at regular intervals.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Overrides BOOTP, the configured IP address, network mask, gateway, hostname, and domain.</td>
</tr>
<tr>
<td><strong>IP Address</strong></td>
<td>Enter the device static IP address. You may enter it alone, in CIDR format, or with an explicit mask. The IP address consists of four octets separated by a period and is used if BOOTP and DHCP are both set to <strong>Off</strong>. Changing this value requires you to reboot the device.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> When DHCP is enabled, the device tries to obtain an IP address from DHCP. If it cannot, the device uses an AutoIP address in the range of 169.254.xxx.xxx.</td>
</tr>
<tr>
<td><strong>Default Gateway</strong></td>
<td>Enter the IP address of the router for this network. Or, clear the field (appears as <code>&lt;None&gt;</code>). This address is only used for static IP address configuration.</td>
</tr>
<tr>
<td><strong>Hostname</strong></td>
<td>Enter the device hostname. It must begin with a letter, continue with a sequence of letters, numbers, and/or hyphens, and end with a letter or number.</td>
</tr>
<tr>
<td><strong>Domain</strong></td>
<td>Enter the device domain name.</td>
</tr>
<tr>
<td><strong>DHCP Client ID</strong></td>
<td>Enter the ID if the DHCP server uses a DHCP ID. The DHCP server’s lease table shows IP addresses and MAC addresses for devices. The lease table shows the Client ID, in hexadecimal notation, instead of the device MAC address.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> &quot;Binary&quot; entry mode allows a mixed mode of text and special characters in brackets. For example, &quot;abcd&lt;ctrl&gt;A&quot; would be entered &quot;abcd[0x01]&quot;.</td>
</tr>
<tr>
<td><strong>Primary DNS</strong></td>
<td>IP address of the primary name server. This entry is required if you choose to configure DNS (Domain Name Server) servers.</td>
</tr>
<tr>
<td><strong>Secondary DNS</strong></td>
<td>IP address of the secondary name server.</td>
</tr>
<tr>
<td><strong>MTU</strong></td>
<td>When DHCP is enabled, the MTU size is (usually) provided with the IP address. When not provided by the DHCP server, or using a static configuration, this value is used. The MTU size can be from 576 to 1500 bytes.</td>
</tr>
</tbody>
</table>

3. Click **Submit** to save changes. Some changes to the following settings require a reboot for the changes to take effect:

- BOOTP Client
- DHCP Client
- IP Address
- DHCP Client ID

**Note:** If DHCP or BOOTP fails, AutoIP intervenes and assigns an address. A new DHCP negotiation is attempted every 5 minutes to obtain a new IP address. When the DHCP is enabled, any configured static IP address is ignored.
Network 1 Ethernet Link

This page shows the current negotiated Ethernet settings and lets you change the speed and duplex settings.

To view and configure the Ethernet link:

1. Click Network on the menu bar and then click Network 1 > Link at the top of the page. The Network 1 (eth0) Ethernet Link page appears.
   - If coming from another Network page, click Network 1 > Link at the top of the page.

   Figure 5-4  Network 1 Ethernet Link

   The Status table shows the current negotiated settings. The Configuration table shows the current range of allowed settings.

2. Enter or modify the following settings:

   Table 5-5  Network 1 Ethernet Link

<table>
<thead>
<tr>
<th>Network 1-Ethernet Link Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Speed</td>
<td>Select the Ethernet link speed. Default is Auto.</td>
</tr>
<tr>
<td>Duplex</td>
<td>Select the Ethernet link duplex mode. Default is Auto.</td>
</tr>
</tbody>
</table>

3. Click Submit. The changes take effect immediately.

   Note: The following section describes the steps to view and configure Line 1 settings; these steps apply to other line instances of the device.
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

Note: The number of lines and tunnels available for viewing and configuration differ between Lantronix products. For example, XPort® Pro embedded networking module and EDS1100 support only one line while other device networking products (such as EDS2100, EDS4100, MatchPort b/g Pro, XPort® AR embedded networking module, EDS8/16PS and EDS8/16/32PR) provide additional lines and tunnels.

Line Settings

View statistics and configure serial interfaces by using the Line web page. Serial interfaces are referred to as lines in this user guide, and a different number of lines, from 1 to 32, may be available for selection depending on your product.

The following sub-menus may be used for a selected line number:

- **Line Statistics**—Displays statistics for the selected line number. 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.

The following sections describe the steps to view and configure specific line number settings. These instructions also apply to additional line instances of the device.

### Line Statistics

This read-only web page shows the status and statistics for the serial line selected at the top of this page.

**Note:** Lines 3 and 4 do not apply for MatchPort AR embedded device server.

1. Select **Line** on the menu bar. The Line web page appears.
2. Select a line number at the top of the page.
3. Select **Statistics**. The Line Statistics page for the selected line appears.
4. Repeat above steps as desired, according to additional line(s) available on your product.

![Figure 6-1 Line 1 Statistics](image)

<table>
<thead>
<tr>
<th>Line 1 - Statistics</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Line</strong></td>
</tr>
<tr>
<td><strong>Statistics</strong></td>
</tr>
<tr>
<td><strong>Bytes:</strong></td>
</tr>
<tr>
<td><strong>Breaks:</strong></td>
</tr>
<tr>
<td><strong>Flow control:</strong></td>
</tr>
<tr>
<td><strong>Parity Errors:</strong></td>
</tr>
<tr>
<td><strong>Framing Errors:</strong></td>
</tr>
<tr>
<td><strong>Overrun Errors:</strong></td>
</tr>
<tr>
<td><strong>No Rx Buffer Errors:</strong></td>
</tr>
<tr>
<td><strong>Queued Receive Bytes:</strong></td>
</tr>
<tr>
<td><strong>Queued Transmit Bytes:</strong></td>
</tr>
<tr>
<td><strong>CTS input:</strong></td>
</tr>
<tr>
<td><strong>RTS output:</strong></td>
</tr>
<tr>
<td><strong>DSR input:</strong></td>
</tr>
<tr>
<td><strong>DTR output:</strong></td>
</tr>
</tbody>
</table>
**Line Configuration**

This page shows the configuration settings for the serial line selected at the top of the page and lets you change the settings for that serial line.

**To configure a specific line:**

1. Select **Line** on the menu bar, if you are not already in the Line web page.
2. Select a line number at the top of the page.
3. Select **Configuration**. The Configuration page for the selected line appears.

![Figure 6-2 Line 1 Configuration](image)

**Line 2 - Configuration**

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name:</td>
<td></td>
</tr>
<tr>
<td>Interface:</td>
<td></td>
</tr>
<tr>
<td>State:</td>
<td>Enabled</td>
</tr>
<tr>
<td>Protocol:</td>
<td>Tunnel</td>
</tr>
<tr>
<td>Baud Rate:</td>
<td>9600</td>
</tr>
<tr>
<td>Parity:</td>
<td>None</td>
</tr>
<tr>
<td>Data Bits:</td>
<td>8</td>
</tr>
<tr>
<td>Stop Bits:</td>
<td>1</td>
</tr>
<tr>
<td>Flow Control:</td>
<td>None</td>
</tr>
<tr>
<td>Xon Char:</td>
<td></td>
</tr>
<tr>
<td>Xoff Char:</td>
<td></td>
</tr>
<tr>
<td>Gap Timer:</td>
<td></td>
</tr>
<tr>
<td>Threshold:</td>
<td></td>
</tr>
</tbody>
</table>
4. Enter or modify the following settings:

<table>
<thead>
<tr>
<th>Line - Configuration Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>If the Terminal Login Menu feature is being used, enter the name for the line. Leaving this field blank will disable this line from appearing in the Terminal Login Menu. The default Name is blank. See Terminal and Host Settings on page 55 for related configuration information.</td>
</tr>
<tr>
<td>Interface</td>
<td>Select the interface type from the drop-down menu. The default is RS232.</td>
</tr>
<tr>
<td>State</td>
<td>Indicates whether the current line is enabled. To change the status, select Enabled or Disabled from the drop-down menu.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Select the protocol from the drop-down menu. The default is Tunnel. <strong>Note:</strong> All protocols work in Connect and Accept Mode except the LPD or Tunnel protocol option which is supported only in Accept Mode.</td>
</tr>
<tr>
<td>Baud Rate</td>
<td>Select the baud rate from the drop-down menu. The default is 9600.</td>
</tr>
<tr>
<td>Parity</td>
<td>Select the parity from the drop-down menu. The default is None.</td>
</tr>
<tr>
<td>Data Bits</td>
<td>Select the number of data bits from the drop-down menu. The default is 8.</td>
</tr>
<tr>
<td>Stop Bits</td>
<td>Select the number of stop bits from the drop-down menu. The default is 1.</td>
</tr>
<tr>
<td>Flow Control</td>
<td>Select the flow control from the drop-down menu. The default is None.</td>
</tr>
<tr>
<td>Xon Char</td>
<td>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.</td>
</tr>
<tr>
<td>Xoff Char</td>
<td>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.</td>
</tr>
<tr>
<td>Gap Timer</td>
<td>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).</td>
</tr>
<tr>
<td>Threshold</td>
<td>The driver will also forward received characters after Threshold bytes have been received.</td>
</tr>
</tbody>
</table>

5. Click **Submit**.

6. Repeat above steps as desired, according to additional line(s) available on your product.
Line Command Mode

Setting the Command Mode enables the CLI on the serial line.

Note: Lines 3 and 4 do not apply for MatchPort AR embedded device server.

To configure Command Mode on a specific line:
1. Select Line on the menu bar, if you are not already in the Line web page.
2. Select a line number at the top of the page.
3. Select Command Mode. The Command Mode page for the selected line appears.

4. Enter or modify the following settings:

<table>
<thead>
<tr>
<th>Line – Command Mode Settings</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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. When the value matches the current value of the group, Command Mode is enabled on the serial line.  
  - **Use both Serial String and CP Group** = the serial string and the value of the CP group must be matched to enable Command Mode.  
  - **Disabled** = turns off Command Mode.  

| Wait Time | Enter the wait time for the serial string during boot-up in milliseconds. |
5. Click **Submit**.

6. Repeat above steps as desired, according to additional line(s) available on your product.

### Tunnel Settings

*Note: The number of lines and tunnels available for viewing and configuration differ between Lantronix products. For example, an XPort Pro and EDS1100 support only one line while other device networking products (such as EDS2100, EDS4100, MatchPort AR, XPort AR, EDS8/16PS and EDS8/16/32PR devices) provide additional lines and tunnels.*

Tunneling allows serial devices to communicate over a network, without “being aware” of the devices which establish the network connection between them. Tunneling parameters are configured using the Web Manager or Command Mode Tunnel Menu. See **Configuration Using Web Manager (on page 24)** or the **MatchPort AR Command Reference** for the full list of commands.

The MatchPort AR embedded device server supports two tunneling connections simultaneously per serial port. One of these connections is Connect Mode; the other connection is Accept Mode. The connections on one serial port are separate from those on another serial port.

* **Connect Mode:** the MatchPort AR embedded device server actively makes a connection. The receiving node on the network must listen for the Connect Mode’s connection. Connect Mode is disabled by default.

* **Accept Mode:** the MatchPort AR device listens for a connection. A node on the network initiates the connection. Accept Mode is enabled by default.

* **Disconnect Mode:** this mode defines how an open connection stops the forwarding of data. The specific parameters to stop the connection are configurable. Once the MatchPort AR Disconnect Mode observes the defined event occur, it will disconnect both Accept Mode and Connect Mode connections on that port.
When any character comes in through the serial port, it gets copied to both the Connect Mode connection and the Accept Mode connection (if both are active).

View statistics and configure a specific tunnel by using the Tunnel web page. When you select Tunnel from the Main Menu, tunnels available for your product will display. Select a specific tunnel to configure.

The following sub-menus listed may be used to configure a specific tunnel:

- **Tunnel – Statistics**
- **Tunnel – Serial Settings**
- **Tunnel – Packing Mode**
- **Tunnel – Accept Mode**
- **Tunnel – Connect Mode**
- **Tunnel – Disconnect Mode**
- **Tunnel – Modem Emulation**

The following sections describe the steps to view and configure specific tunnel number settings. These instructions also apply to additional tunnel menu options.

### Tunnel – Statistics

The MatchPort AR embedded device server logs statistics for tunneling. The **Dropped** statistic shows connections ended by the remote location. The **Disconnects** statistic shows connections ended by the MatchPort AR unit.

To display statistics for a specific tunnel:

1. Select **Tunnel** on the menu bar. The Tunnel web page appears.
2. Select a tunnel number at the top of the page.
3. Select **Statistics**. The Tunnel Statistics page for the specific tunnel appears.

   If a particular tunnel is connected, the following becomes available:

   - Identifying information about the tunnel connection (i.e., “Connect 1 Counters”)
   - Address of connection (i.e., “local:10001 -> 172.22.22.22.10001”)
   - **Kill Connection(s)** link: Click this link to terminate this active tunnel connection, as desired.
   - Octets forwarded from Serial
   - Octets forwarded from Network
   - Uptime
4. Repeat above steps as desired, according to additional tunnel(s) available on your product.

**Figure 6-6 Tunnel 1 Statistics**

<table>
<thead>
<tr>
<th>Tunnel 1</th>
<th>Tunnel 2</th>
<th>Tunnel 3</th>
<th>Tunnel 4</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Statistics</strong></td>
<td><strong>Serial Settings</strong></td>
<td><strong>Packing Mode</strong></td>
<td><strong>Modem Emulation</strong></td>
</tr>
<tr>
<td>Accept Mode</td>
<td>Connect Mode</td>
<td>Disconnect Mode</td>
<td></td>
</tr>
</tbody>
</table>

**Tunnel 1 - Statistics**

<table>
<thead>
<tr>
<th>Aggregate Counters</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Completed Accepts</td>
<td>0</td>
</tr>
<tr>
<td>Completed Connects</td>
<td>0</td>
</tr>
<tr>
<td>Disconnects</td>
<td>0</td>
</tr>
<tr>
<td>Dropped Accepts</td>
<td>0</td>
</tr>
<tr>
<td>Dropped Connects</td>
<td>0</td>
</tr>
<tr>
<td>Octets forwarded from Serial</td>
<td>0</td>
</tr>
<tr>
<td>Octets forwarded from Network</td>
<td>0</td>
</tr>
<tr>
<td>Accept Connection Time</td>
<td>0 days 00:00:00</td>
</tr>
<tr>
<td>Connect 1 Connection Time</td>
<td>0 days 00:00:00</td>
</tr>
<tr>
<td>Connect 2 Connection Time</td>
<td>0 days 00:00:00</td>
</tr>
<tr>
<td>Connect 3 Connection Time</td>
<td>0 days 00:00:00</td>
</tr>
<tr>
<td>Connect 4 Connection Time</td>
<td>0 days 00:00:00</td>
</tr>
<tr>
<td>Connect 5 Connection Time</td>
<td>0 days 00:00:00</td>
</tr>
<tr>
<td>Connect 6 Connection Time</td>
<td>0 days 00:00:00</td>
</tr>
<tr>
<td>Connect 7 Connection Time</td>
<td>0 days 00:00:00</td>
</tr>
<tr>
<td>Connect 8 Connection Time</td>
<td>0 days 00:00:00</td>
</tr>
<tr>
<td>Connect DNS Address Changes</td>
<td>0</td>
</tr>
<tr>
<td>Connect DNS Address Invalids</td>
<td>0</td>
</tr>
</tbody>
</table>

**Accept Counters**

<table>
<thead>
<tr>
<th>Line</th>
<th>Counters</th>
<th>Stats</th>
<th>Kill Connection[s]</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Connect 1 Counters</td>
<td></td>
<td>local:10001 -&gt; 172.19.213.84:10001</td>
</tr>
<tr>
<td>2</td>
<td>Connect 2 Counters</td>
<td></td>
<td>Octets forwarded from Serial: 10369</td>
</tr>
<tr>
<td>3</td>
<td>Connect 3 Counters</td>
<td></td>
<td>Octets forwarded from Network: 31107</td>
</tr>
<tr>
<td>4</td>
<td>Connect 4 Counters</td>
<td></td>
<td>Uptime: 6 days 00:40:44</td>
</tr>
<tr>
<td>5</td>
<td>Connect 5 Counters</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Connect 6 Counters</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Connect 7 Counters</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Connect 8 Counters</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Note:** Lines 3 and 4 do not apply for MatchPort AR embedded device server.

**Additional information appears for each active tunnel connection including a link allowing you to terminate the connection.**
Tunnel – Serial Settings
Serial line settings are configurable for the corresponding serial line of the specific tunnel. Configure the buffer size to change the maximum amount of data the serial port stores. For any active connection, the device sends the data in the buffer.

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

To configure serial settings for a specific tunnel:

1. Select **Tunnel** on the menu bar, if you are not already in the Tunnel web page.
2. Select a tunnel number at the top of the page.
3. Select **Serial Settings**. The Serial Settings page for the specific tunnel appears.

Figure 6-7 Tunnel 1 Serial Settings

![Tunnel 1 Serial Settings](image)

**Note:** Lines 3 and 4 do not apply for MatchPort AR embedded device server.

4. View or modify the following settings:

Table 6-8  Tunnel - Serial Settings

<table>
<thead>
<tr>
<th><strong>Tunnel - Serial Settings</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Line Settings</strong> (display only)</td>
<td>Current serial settings for the line.</td>
</tr>
<tr>
<td><strong>Protocol</strong> (display only)</td>
<td>The protocol being used on the line. In this case, Tunnel.</td>
</tr>
</tbody>
</table>
6. Click **Submit**.

5. Repeat above steps as desired, according to additional tunnel(s) available on your product.

### Tunnel – Packing Mode

Packing Mode takes data from the serial port, packs it together, and sends it 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 Packing Mode for a specific tunnel:**

1. Select **Tunnel** on the menu bar, if you are not already in the Tunnel web page.
2. Select a tunnel number at the top of the page.
3. Select **Packing Mode**. The Packing Mode page for the specific tunnel appears.

**Note:** Lines 3 and 4 do not apply for MatchPort AR embedded device server.

<table>
<thead>
<tr>
<th>Tunnel - Serial Settings</th>
<th>Description</th>
</tr>
</thead>
</table>
| **DTR**                  | Select when to assert DTR.  
  - **Unasserted** = never asserted  
  - **TruPort** = asserted whenever either a connect or an accept mode tunnel connection is active with the Telnet Protocol RFC2217 saying that the remote DSR is asserted.  
  - **Asserted while connected** = asserted whenever either a connect or an accept mode tunnel connection is active.  
  - **Continuously asserted** = asserted regardless of the status of a tunnel connection. |
Depending on the Mode selection, different configurable parameters for the specific tunnel number are presented to the user. The following figures show the display for each of the three packing modes.

**Note:** Lines 3 and 4 do not apply for MatchPort AR embedded device server for Figure 6-10 and Figure 6-11.

4. Enter or modify the following settings:
Table 6-12 Tunnel Packing Mode

<table>
<thead>
<tr>
<th>Tunnel - Packing Mode Settings</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Mode**                     | - Select **Disable** to disable Packing Mode completely.  
- Select **Timeout** to send data after the specified time has elapsed.  
- Select **Send Character** to send the queued data when the send character is received. |
| **Threshold** (Appears for both Timeout and Send Character Modes) | Send the queued data when the number of queued bytes reaches the threshold. When the buffer fills to this specified amount of data in bytes (and the timeout has not elapsed), the device packs the data and sends it out; applies only if the Packing Mode is not Disabled. |
| **Timeout** (Appears for Timeout Mode) | Enter a time, in milliseconds, for the device to send the queued data after the first character was received. Specifies the time duration in milliseconds; applies only if the Packing Mode is Timeout. |
| **Send Character** (Appears for Send Character Mode) | Enter the send character (single printable or control). Upon receiving this character, the device sends out the queued data. The data is packed until the specified send character is encountered. Similar to a start or stop character, the device packs the data until it sees the send character. The device then sends the packed data and the send character in the packet. Applies only if the Packing Mode is Send Character. |
| **Trailing Character** (Appears for Send Character Mode) | Enter the trailing character (single printable or control). This character is sent immediately following the send character. This is an optional setting. If a trailing character is defined, this character is appended to data put on the network immediately following the send character. |

5. Click **Submit**.
6. Repeat above steps as desired, according to additional tunnel(s) available on your product.

**Tunnel – Accept Mode**

Controls how a specific tunnel number behaves when a connection attempt originates from the network. In Accept Mode, the MatchPort AR embedded device server 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 increases sequentially for each additional serial port, if supported.

Accept Mode supports the following protocols:

- SSH (the MatchPort AR device is the server in Accept Mode). When using this protocol, the SSH server host keys and at least one SSH authorized user must be configured.
- SSL
- TCP
- AES encryption over TCP
- Telnet (the MatchPort AR embedded device server 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 (when the modem control pin is asserted on the serial line corresponding to the tunnel)
- Modem emulation

To configure the Accept Mode of a specific tunnel:

1. Select Tunnel on the menu bar, if you are not already in the Tunnel web page.
2. Select a tunnel number at the top of the page.
3. Select Accept Mode. The Accept Mode page for the specific tunnel appears.

   **Figure 6-13 Tunnel 1 Accept Mode**

4. Enter or modify the following settings:

   **Table 6-14 Tunnel Accept Mode**

<table>
<thead>
<tr>
<th>Tunnel - Accept Mode Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Mode</strong></td>
<td>Select the method used to start a tunnel in Accept mode. Choices are:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Disabled</strong> = do not accept an incoming connection.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Always</strong> = accept an incoming connection (<strong>default</strong>)</td>
</tr>
<tr>
<td></td>
<td>- <strong>Any Character</strong> = start waiting for an incoming connection when any character is read on the serial line.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Start Character</strong> = start waiting for an incoming connection when the start character for the specific tunnel is read on the serial line.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Modem Control Asserted</strong> = 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.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Modem Emulation</strong> = start waiting for an incoming connection when triggered by modem emulation AT commands. Connect mode must also be set to Modem Emulation.</td>
</tr>
<tr>
<td><strong>Local Port</strong></td>
<td>Enter the port number for use as the local port. The defaults are port 10001 for Tunnel 1. Additional tunnels, if supported, increase sequentially.</td>
</tr>
<tr>
<td><strong>Protocol</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>TCP Keep Alive</strong></td>
<td>Enter the time, in seconds, the device 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.</td>
</tr>
<tr>
<td><strong>Flush Serial Data</strong></td>
<td>Select Enabled to flush the serial data buffer on a new connection.</td>
</tr>
<tr>
<td><strong>Block Serial Data</strong></td>
<td>Select On to block, or not tunnel, serial data transmitted to the device.</td>
</tr>
<tr>
<td><strong>Block Network</strong></td>
<td>Select On to block, or not tunnel, network data transmitted to the device.</td>
</tr>
</tbody>
</table>
5. Click **Submit**.

6. Repeat above steps as desired, according to additional tunnel(s) available on your product.

<table>
<thead>
<tr>
<th><strong>Tunnel - Accept Mode Settings (continued)</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Password</strong></td>
<td>Enter a password that clients must send to the device 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 device must be terminated with one of the following: (a) 0x0A (LF), (b) 0x00, (c) 0x0D 0x0A (CR LF), or (d) 0x0D 0x00.</td>
</tr>
<tr>
<td><strong>Email on Connect</strong></td>
<td>Select whether the device 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.</td>
</tr>
<tr>
<td><strong>Email on Disconnect</strong></td>
<td>Select whether the device 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.</td>
</tr>
</tbody>
</table>
| **CP Output**                               | Identifies a CP or 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. |
Tunnel – Connect Mode

Connect Mode defines how the device makes an outgoing connection through a specific tunnel. When enabled, Connect Mode is always on and attempting a network connection if the connection mode condition warrants it. For Connect Mode to function, it must:

- Be enabled
- Have a remote host configured
- Have a remote port configured

Enter the remote host address as an IP address or DNS name. The MatchPort AR device will make a connection only if it can resolve the address. For DNS names, the MatchPort AR embedded device server will re-evaluate the address after being established for 4 hours. If re-evaluation results in a different address, it will close the connection.

Connect Mode supports the following protocols:

- **TCP**
- **AES encryption over TCP and UDP**
  
  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.
- **SSH**
  
  To configure SSH, the SSH client username must be configured. In Connect Mode, the AR unit is the SSH client. Ensure the MatchPort AR SSH client username is configured on the remote SSH server before using it with the MatchPort AR embedded device server.
- **SSL**
- **UDP**
  
  Is only available in Connect Mode because it is a connectionless protocol. For Connect Mode using UDP, the MatchPort AR unit accepts packets from any device on the network. It will send packets to the last device that sent it packets.
- **Telnet**

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

There are six different connect modes:

- **Disable**
  
  No connection is attempted.
- **Always**
  
  A connection is always attempted.
- **Any Character**
  
  A connection is attempted if it detects any character from the serial port.
- **Start Character**
  
  A connection is attempted if it detects a specific and configurable character from the serial port.

**Note:** While in the “Any Character” or “Start Character” connection modes, the MatchPort AR embedded device server waits and retries the connection if the connection cannot be made. Once it makes a connection and then disconnects, it will not reconnect until it sees another character or the start character again (depending on the configured setting).
Modem Control Asserted
A connection is attempted when the modem control pin is asserted in the serial line.

**Note:** Configure the Modem Control Asserted setting (for DSR or DTR) to start a Connect Mode connection when the signal is asserted. The MatchPort AR embedded device server 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 by an ATD command.

**To configure Connect Mode for a specific tunnel:**

1. Select **Tunnel** on the menu bar, if you are not already in the Tunnel web page.
2. Select a tunnel number at the top of the page.
3. Select **Connect Mode**. The Connect Mode page for the specific tunnel appears.

---

**Figure 6-15 Tunnel 1 - Connect**

<table>
<thead>
<tr>
<th>Statistics</th>
<th>Serial Settings</th>
<th>Packing Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accept Mode</td>
<td>Connect Mode</td>
<td>Disconnect Mode</td>
</tr>
</tbody>
</table>

**Tunnel 2 - Connect Mode**

- **Mode:** Disable
- **Local Port:** <Random>
- **Host 1:** <None>
- **Reconnect Timer:** 15000 milliseconds
- **Flush Serial Data:** Enabled
- **Block Serial:** Enabled
- **Block Network:** Enabled
- **Email on Connect:** <None>
- **Email on Disconnect:** <None>
- **CP Output:** Group:
4. Enter or modify the following settings:

### Table 6-16  Tunnel Connect Mode

<table>
<thead>
<tr>
<th>Tunnel – Connect Mode Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Mode</strong></td>
<td>Select the method to be used to attempt a connection to a remote host or device. Choices are:&lt;br&gt;🔹 <strong>Always</strong> = a connection is attempted until one is made. If the connection gets disconnected, the MatchPort AR embedded device server retries until it makes a connection. (default)&lt;br&gt;🔹 <strong>Disable</strong> = an outgoing connection is never attempted.&lt;br&gt;🔹 <strong>Any Character</strong> = a connection is attempted when any character is read on the serial line.&lt;br&gt;🔹 <strong>Start Character</strong> = a connection is attempted when the start character for the specific tunnel is read on the serial line.&lt;br&gt;🔹 <strong>Modem Control Asserted</strong> = a connection is attempted as long as the Modem Control pin (DSR) is asserted, until a connection is made.&lt;br&gt;🔹 <strong>Modem Emulation</strong> = a connection is attempted when triggered by modem emulation AT commands.</td>
</tr>
<tr>
<td><strong>Local Port</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Host</strong></td>
<td>Click <code>&lt;None&gt;</code> in the Host field to configure the Host parameters.&lt;br&gt;🔹 <strong>Address</strong> = Enter the remote Host Address as an IP address or DNS name. It designates the address of the remote host to connect to. Displays configured IP address or DNS address.&lt;br&gt;🔹 <strong>Port</strong> = Enter the port for use as the Host Port. It designates the port on the remote host to connect to. Displays configured Port.&lt;br&gt;🔹 <strong>Protocol</strong> = Select the protocol type for use with Connect Mode. The default protocol is TCP. Additional fields may need to be completed depending on protocol chosen for the host:&lt;br&gt;🔹 For <strong>SSH</strong>, also enter an <strong>SSH Username</strong>.&lt;br&gt;🔹 For <strong>SSL</strong>, also select Enabled or Disabled for <strong>Validate Certificate</strong>.&lt;br&gt;🔹 For <strong>SSL</strong>, <strong>TCP</strong>, <strong>TCP AES</strong> and <strong>Telnet</strong>, use the <strong>TCP Keep Alive</strong> field to adjust the value.&lt;br&gt;🔹 For <strong>TCP AES</strong>, enter the <strong>AES Encrypt</strong> and <strong>AES Decrypt Keys</strong>. Both of keys may be set to the same value.&lt;br&gt;🔹 For <strong>UDP</strong>, there are no additional fields to complete. In this mode, the device accepts packets from any device on the network and sends packets to the last device that sent it packets.&lt;br&gt;🔹 For <strong>UDP AES</strong>, enter the <strong>AES Encrypt</strong> and <strong>AES Decrypt Keys</strong>.&lt;br&gt;🔹 <strong>SSH Username</strong> = Displays configured username, used only if SSH protocol is selected.&lt;br&gt;🔹 <strong>TCP Keep Alive</strong> = Default is 45000 milliseconds. Enter zero to disable and blank the value to restore the default.&lt;br&gt;🔹 <strong>AES Encrypt/Decrypt Key</strong> = Displays presence of key, used only if protocol with AES is selected.</td>
</tr>
</tbody>
</table>

*Note: If security is a concern, it is highly recommended that SSH be used. When using SSH, both the SSH Server Host Keys and SSH Server Authorized Users must be configured.*
## 6: Line and Tunnel Settings

<table>
<thead>
<tr>
<th><strong>Tunnel – Connect Mode Settings (continued)</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Reconnect Timer</strong></td>
<td>Enter the reconnect time in milliseconds. The device attempts to reconnect after this amount of time after failing a connection or exiting an existing connection. This behavior depends upon the Disconnect Mode.</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td></td>
</tr>
<tr>
<td>✦ When you configure <strong>Tunnel - Connect Mode</strong>, you can specify a number of milliseconds to attempt to reconnect after a dropped connection has occurred. The default is 1500 milliseconds.</td>
<td></td>
</tr>
<tr>
<td>✦ The <strong>Reconnect Timer</strong> only applies if a <strong>Disconnect Mode</strong> is configured. With a <strong>Disconnect Mode</strong> 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.</td>
<td></td>
</tr>
<tr>
<td>✦ Any network-side disconnect is considered an error and a reconnect is attempted without regard to the <strong>Connect Mode</strong> settings. Simultaneous <strong>Connect Mode</strong> connections require some <strong>Disconnect Mode</strong> configurations or the connections will never terminate. See <strong>Tunnel – Disconnect Mode</strong> on page 50 for more information about the parameters.</td>
<td></td>
</tr>
<tr>
<td>✦ If <strong>Disconnect Mode</strong> is disabled and the network connection is dropped, then the re-establishment of a tunnel connection is governed by the configured <strong>Connect Mode</strong> settings.</td>
<td></td>
</tr>
<tr>
<td><strong>Flush Serial Data</strong></td>
<td>Select whether to flush the serial line when a connection is made. Choices are:</td>
</tr>
<tr>
<td>✦ <strong>Enabled</strong> = flush the serial line when a connection is made.</td>
<td></td>
</tr>
<tr>
<td>✦ <strong>Disabled</strong> = do not flush the serial line. (default)</td>
<td></td>
</tr>
<tr>
<td><strong>Block Serial</strong></td>
<td>Select <strong>Enabled</strong> to block (not tunnel) serial data transmitted to the device. This is a debugging tool that causes serial data sent to the device to be ignored.</td>
</tr>
<tr>
<td><strong>Block Network</strong></td>
<td>Select <strong>Enabled</strong> to block (not tunnel) network data transmitted to the device. This is a debugging tool that causes network data sent to the device to be ignored.</td>
</tr>
<tr>
<td><strong>Email on Connect</strong></td>
<td>Select whether the device 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.</td>
</tr>
<tr>
<td><strong>Email on Disconnect</strong></td>
<td>Select whether the device 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.</td>
</tr>
<tr>
<td><strong>CP Output</strong></td>
<td>Identifies a CP or CP Group whose value should change when a connection is established and when it is dropped.</td>
</tr>
<tr>
<td>✦ <strong>Connection value</strong>—Specifies the value to set the CP Group to when a connection is established.</td>
<td></td>
</tr>
<tr>
<td>✦ <strong>Disconnection value</strong>—Specifies the value to set the CP Group to when the connection is closed.</td>
<td></td>
</tr>
</tbody>
</table>

5. **Click Submit.** The host is configured. Repeat these steps to configure additional hosts as necessary. MatchPort AR supports configuration of up to sixteen hosts.
Connecting Multiple Hosts

If more than one host is configured, a Host Mode option appears. Host Mode controls how multiple hosts will be accessed. For MatchPort AR embedded device server, the Connect Mode supports up to sixteen Hosts. Hosts may be accessed sequentially or simultaneously:

- **Sequential** – 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 (see **Host List Promotion on page 50**). Sequential is the default Host Mode.

- **Simultaneous** – A tunnel will connect to all hosts accepting a connection. Connections occur at the same time to all listed hosts. The device can support a maximum of 64 total aggregate connections.

Host List Promotion

This feature allows Host IP promotion of individual hosts in the overall sequence.

To promote a specific Host:

1. Click the icon in the desired Host field, for example Host 2 and Host 3.
2. The selected Host(s) exchanges its place with the Host above it.
3. Click Submit. The hosts change sequence.

Tunnel – Disconnect Mode

Relates to the disconnection of a specific tunnel. Disconnect Mode ends Accept Mode and Connect Mode connections. When disconnecting, the MatchPort AR unit shuts down the specific tunnel connection gracefully.

The following settings end a specific tunnel connection:

- The MatchPort AR embedded device server receives the stop character.
6: Line and Tunnel Settings

- The timeout period has elapsed and no activity is going in or out of the MatchPort AR device. Both Accept Mode and Connect Mode must be idle for the time frame.

- The MatchPort AR unit observes the modem control inactive setting.

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

**To configure the Disconnect Mode for a specific tunnel:**

1. Select **Tunnel** on the menu bar, if you are not already in the Tunnel web page.
2. Select a tunnel number at the top of the page.
3. Select **Disconnect Mode**. The specific tunnel Disconnect Mode page appears.

**Note:** Lines 3 and 4 do not apply for MatchPort AR embedded device server.

4. Enter or modify the following settings:

- **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 device 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.

5. Click **Submit**.

6. Repeat above steps as desired, according to additional tunnel(s) available on your product.
Tunnel – Modem Emulation

A tunnel in Connect Mode can be initiated using modem commands incoming from the Serial Line. This page enables you to configure the modem emulation settings when you select Modem Emulation as the Tunnel Connect Mode type. 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 embedded device server, an “OK” message is sent (but the command is silently ignored).

The MatchPort AR unit 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.

The following table lists and describes the available commands.

**Table 6-20  Modem Emulation Commands and Descriptions**

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

1. Select **Tunnel** on the menu bar, if you are not already in the Tunnel web page.
2. Select a tunnel number at the top of the page.
3. Select **Modem Emulation**. The Modem Emulation page for the specific tunnel appears.

4. Enter or modify the following settings:

![Tunnel 1 Modem Emulation](image)

**Tunnel 2 - Modem Emulation**

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Echo Pluses</td>
<td>Enabled/Disabled</td>
</tr>
<tr>
<td>Echo Commands</td>
<td>Enabled/Disabled</td>
</tr>
<tr>
<td>Verbose Response</td>
<td>Enabled/Disabled</td>
</tr>
<tr>
<td>Response Type</td>
<td>Text</td>
</tr>
<tr>
<td>Error Unknown Commands</td>
<td>Enabled/Disabled</td>
</tr>
<tr>
<td>Incoming Connection</td>
<td>Disabled/Manual</td>
</tr>
<tr>
<td>Connect String</td>
<td></td>
</tr>
<tr>
<td>Display Remote IP</td>
<td>Enabled/Disabled</td>
</tr>
</tbody>
</table>
Table 6-22 Tunnel Modem Emulation

<table>
<thead>
<tr>
<th>Tunnel-Modem Emulation Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Echo Pluses</td>
<td>Select <strong>Enabled</strong> to echo +++ when entering modem Command Mode.</td>
</tr>
<tr>
<td>Echo Commands</td>
<td>Select <strong>Enabled</strong> to echo the modem commands to the console.</td>
</tr>
<tr>
<td>Verbose Response</td>
<td>Select <strong>Enabled</strong> to send modem response codes out on the serial line.</td>
</tr>
<tr>
<td>Response Type</td>
<td>Select the type of response code: <strong>Text</strong> or <strong>Numeric</strong>.</td>
</tr>
</tbody>
</table>
| 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**. |
| 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**. |

5. Click **Submit**.

6. Repeat above steps as desired, according to additional tunnel(s) available on your product.
7:  Terminal and Host Settings

This chapter describes how to view and configure the Terminal Login Connect Menu and associated Host configuration. It contains the following sections:

- Terminal Settings
- Host Configuration

The Terminal Login Connect Menu feature allows the MatchPort AR embedded device server to present a menu of predefined connections when the device is accessed via telnet, ssh, or a serial port. From the menu, a user can choose one of the presented options and the device automatically makes the predefined connection.

The Terminal page controls whether a Telnet, SSH, or serial port connection presents the CLI or the Login Connect Menu. By default, the CLI is presented when the device is accessed. When configured to present the Login Connect Menu, the hosts configured via the Hosts page, and named serial lines are presented.

Terminal Settings

This page shows configuration settings for each terminal connection method. You can configure whether each serial line or the telnet/SSH server presents a CLI or a Login Connect menu when a connection is made.

Network Terminal Configuration

To configure menu features applicable to CLI access via the network:

1. Select Terminal on the menu bar, if you are not already in the Terminal web page.
2. Select Network at the top of the page. The Configuration submenu is automatically selected. The Terminal Configuration page appears for the network.

3. Enter or modify the following settings:

![Figure 7-1 Terminal on Network Configuration](image)

<table>
<thead>
<tr>
<th>Terminal on Network - Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Terminal Type:</strong></td>
</tr>
<tr>
<td><strong>Login Connect Menu:</strong></td>
</tr>
<tr>
<td><strong>Exit Connect Menu:</strong></td>
</tr>
<tr>
<td><strong>Echo:</strong></td>
</tr>
</tbody>
</table>
Table 7-2  Terminal on Network Configuration

<table>
<thead>
<tr>
<th>Terminal on Network Configuration Settings</th>
<th>Description</th>
</tr>
</thead>
</table>
| Terminal Type | Enter text to describe the type of terminal. The text will be sent to a host via IAC.  
Note: IAC means, “interpret as command.” It is a way 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. |
| 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. |

4. Click Submit to save changes.

Line Terminal Configuration

To configure a specific line to support an attached terminal:

1. Select Terminal on the menu bar. The Terminal web page appears.
2. Select the line number at the top of the page connected to the terminal you want to configure. The default is Line 1.

![Figure 7-3 Terminal on Line Configuration](image)

3. Enter or modify the following settings:
Table 7-4  Terminal on Line 1 Configuration

<table>
<thead>
<tr>
<th>Terminal on Line Configuration Settings</th>
<th>Description</th>
</tr>
</thead>
</table>
| Terminal Type                          | Enter text to describe the type of terminal. The text will be sent to a host via IAC.  
   Note: IAC means, “interpret as command.” It is a way 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. |
| 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. |

4. Click Submit to save changes.
5. Repeat above steps as desired, according to the additional line(s) available on your product.

Host Configuration

This Host web page is where you may view and modify current settings for a selected remote host.

To configure a selected remote host:
1. Select Host on the menu bar. The Host web page appears.
2. Select a specific host number at the top of the page. The Host Configuration page for the selected host appears.

Note: Number of hosts available differ among Lantronix products. Hosts available for selection may appear listed on the screen (see Figure 7-5) or within a drop-down menu above the Configuration button.
3. Enter or modify the following settings:

**Table 7-6  Host Configuration**

<table>
<thead>
<tr>
<th>Host Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>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.</td>
</tr>
</tbody>
</table>
| 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 device will connect. |
| Remote Port   | Enter the port on the host to which the device will connect. |

4. Click **Submit** to save changes.

5. Repeat above steps as desired, according to additional host(s) available on your product.
8: **Configurable Pin Manager**

The Configurable Pin Manager is responsible for assignment and control of the configurable pins (CPs) available on the MatchPort AR embedded device server. There are seven configurable pins on the MatchPort AR unit.

You can configure the CPs by making them part of a group. A CP Group may consist of one or more CPs. This increases flexibility when incorporating the MatchPort AR embedded device server into another system.

This chapter contains the following sections:

- **Overview**
- **CPM: CP (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**

MatchPort AR unit 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 device 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.

**CPM: CP (Configurable Pins)**

Each CP is associated with an external hardware pin. CPs can trigger an outside event, like sending an email message or starting Command Mode on a serial Line.
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, use the CPM Groups web page. See CPM: Groups on page 62.

**View CPs**

1. Select CPM on the menu bar and then CPs at the top of the page. The CPM: CPs page appears.

![Figure 8-1 CPM: CPs](image)

The Current Configuration table shows the current settings for each CP.
Table 8-2  CPM CPs Current Configuration

<table>
<thead>
<tr>
<th>CPM – CPs Current Configuration</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CP</td>
<td>Indicates the configurable pin number.</td>
</tr>
<tr>
<td>Ref</td>
<td>Indicates the hardware pin number associated with the CP.</td>
</tr>
<tr>
<td>Configured As</td>
<td>Shows the CP configuration. A CP configured as <strong>Input</strong> is set to read input. A CP configured as <strong>Output</strong> drives data out of the device.</td>
</tr>
</tbody>
</table>
| Value                           | Indicates the current status of the CP:  
  ◆ 1 = asserted  
  ◆ 0 = de-asserted  
  ◆ Inv = the CP logic is inverted |
| 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. |

2. Select a CP number (CP column) in the Current Configuration table to display the status of that pin. The CP Status table shows the information about the CP.

Table 8-3  CPM CPs Status

<table>
<thead>
<tr>
<th>CPM – CPs Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Shows the CP number.</td>
</tr>
<tr>
<td>State</td>
<td>Shows the current enable state of the CP.</td>
</tr>
<tr>
<td>Type</td>
<td>Indicates whether the CP is set for input or output.</td>
</tr>
<tr>
<td>Value</td>
<td>Shows the last bit in the CP current value.</td>
</tr>
<tr>
<td>Bit</td>
<td>Visual display of the 32 bit placeholders for a CP.</td>
</tr>
<tr>
<td>Level</td>
<td>A “+” symbol indicates the CP is asserted (the voltage is high). A “-” indicates the CP voltage is low.</td>
</tr>
</tbody>
</table>
| I/O              | Indicates the current status of the pin:  
  ◆ I = input  
  ◆ O = output  
  ◆ <blank> = unassigned |
| Logic            | An “I” indicates the CP is inverted. |
| 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.

To change a CP output value:
1. Select the CP number (in CP column) from the current configuration table.
2. Enter the CP value in the CP Status table.
3. Click **Set**. The changed CP value appears in the current configuration table.
To change a CP configuration:
1. Select the CP number (in CP column) from the current configuration table.
2. Select the CP configuration from the Type drop-down list in the CP Status table.
3. (If necessary) Select the Assert Low checkbox.
4. Click Change.

*Note:* These changes to a CP are not saved in FLASH. Instead, these settings are used when the CP is added to a CP Group. When the CP Group is saved, its CP settings are saved with it. Thus, a particular CP may be defined as “Input” in one group but as “Output” in another. Only one group containing a particular CP may be enabled at once.

### CPM: Groups

The CP Groups page allows for the adding, removing and managing of CP groups. Groups can be created or deleted. CPs can be added to or removed from 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 Groups

1. Select CPM on the menu bar and then Groups at the top of the page. The CPM: Groups page appears.

   ![Figure 8-4 CPM: Groups](image)

2. The Current Configuration table shows the current settings for each CP group.

<table>
<thead>
<tr>
<th>CPM – Groups Current Configuration</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group (Name)</td>
<td>Shows the CP group’s name.</td>
</tr>
<tr>
<td>State</td>
<td>Indicates whether the group is enabled or disabled.</td>
</tr>
<tr>
<td>CP Info</td>
<td>Indicates the number of CPs assigned to this particular group.</td>
</tr>
</tbody>
</table>
To display the status of a specific group:
1. Select **CPM > Groups**.
2. Select the CP group name in the Current Configuration table.

### CPM: Groups

#### Current Configuration

<table>
<thead>
<tr>
<th>Group Name</th>
<th>State</th>
<th>CP Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Enabled</td>
<td>0 CPs Assigned</td>
</tr>
<tr>
<td>2C</td>
<td>Disabled</td>
<td>2 CPs Assigned</td>
</tr>
<tr>
<td>Line1_Modem_CTL_In</td>
<td>Disabled</td>
<td>0 CPs Assigned</td>
</tr>
<tr>
<td>Line1_Modem_CTL_O</td>
<td>Disabled</td>
<td>0 CPs Assigned</td>
</tr>
<tr>
<td>Line1_RS485_HDpx</td>
<td>Enabled</td>
<td>1 CP Assigned</td>
</tr>
<tr>
<td>Line1_RS485_Select</td>
<td>Enabled</td>
<td>1 CP Assigned</td>
</tr>
<tr>
<td>Line2_Modem_CTL_In</td>
<td>Disabled</td>
<td>0 CPs Assigned</td>
</tr>
<tr>
<td>Line2_Modem_CTL_O</td>
<td>Disabled</td>
<td>0 CPs Assigned</td>
</tr>
<tr>
<td>Modbus_CTL_In</td>
<td>Disabled</td>
<td>0 CPs Assigned</td>
</tr>
<tr>
<td>Modbus_CTL_Out</td>
<td>Disabled</td>
<td>0 CPs Assigned</td>
</tr>
<tr>
<td>output</td>
<td>Enabled</td>
<td>1 CP Assigned</td>
</tr>
</tbody>
</table>

#### Create Group:

#### Group Status

**Name**: Line1_Modem_CTL_O

**State**: Disabled AND Locked, user may Enable/Disable or Add/Remove CP

**Value**: Disabled

**Bit**: 6 5 4 3 2 1 0

**I/O**:

**Logic**

**Binary**: x x x x x x x x

**CP#**

Table 8-7  Group Status

<table>
<thead>
<tr>
<th><strong>CPM – Groups Page</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Group Status</strong></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Shows the CP Group name.</td>
</tr>
<tr>
<td>State</td>
<td>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.</td>
</tr>
<tr>
<td>Value</td>
<td>Shows the CP group’s current value.</td>
</tr>
</tbody>
</table>
To create a custom CP group:
1. Select **CPM > Groups**.
2. Enter a group name in the **Create Group** field.
3. Click **Submit**.

To add a CP to a Group
1. Select **CPM > Groups**.
2. Select a specific **Group Name** to select it. The Group Status information for the group appears in a table below the current configuration.
3. Select a CP from the drop-down list beneath the Group Status table.
4. Select a bit position from the drop-down list.
5. Select Input or Output from the drop-down list.
6. Check the Assert Low checkbox to specify negative logic (inverted assertion), as desired. This box is unchecked by default.
7. Click **Add** to complete adding the CP to the group.

To delete a custom CP group:
1. Select **CPM > Groups**.
2. Select a custom CP Group Name from the drop-down list beside the current configuration table.
3. Click the red X next to the corresponding Name in the Group Status table.

To enable or disable a CP group:
1. Select **CPM > Groups**.
2. Select the Group name in the table representing the group you wish to enable. The Group Status information for this group appears in a table below.
3. Click **Enable** to enable, as appropriate.
4. Click **Disable** to disable, as appropriate.

<table>
<thead>
<tr>
<th>CPM – Groups Page Group Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bit</td>
<td>Displays the individual bit positions for the available CPs.</td>
</tr>
<tr>
<td>Level</td>
<td>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.</td>
</tr>
</tbody>
</table>
| I/O                           | Indicates the current status of the pin:  

- I = input  
- O = output  
- <blank> = unassigned |
| Logic                         | Indicates the logic level of the CP. An "I" indicates the CP 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 group is disabled or the bit is unassigned in the group. |
| CP#                           | Shows the configurable pin number and its bit position in the CP group. |
To set a CP group’s value:
1. Create a custom group and add a CP to it.
2. Select **CPM > Groups**.
3. Select the custom group from the current configuration table.
4. Enter a **Group Status Value**.
5. Click **Set**.

To remove a CP from a Group:
1. Select **CPM > Groups**.
2. Select a the group in the Group Name column that contains the CP to be removed.
3. Select the CP from the drop-down list beside the **Remove** button.
4. Click **Remove**.
9: **Service Settings**

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

- **DNS Settings**
- **Point-to-Point (PPP) Settings**
- **SNMP Settings**
- **FTP Settings**
- **TFTP Settings**
- **Syslog Settings**
- **HTTP Settings**
- **RSS Settings**
- **LPD Settings**

**DNS Settings**

The primary and secondary domain name system (DNS) addresses come from the active interface. The static addresses from the Network Interface Configuration 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 are stored in the DNS cache temporarily. The MatchPort AR checks this cache when performing forward lookups. Each item in the cache eventually times out and is removed automatically after a certain period, or you can delete it manually.

**To view the DNS status:**

1. Select DNS on the menu bar. The DNS page appears.

![Figure 9-1 DNS Settings](image-url)

**DNS**

<table>
<thead>
<tr>
<th>Current Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain: eng.lantronix.com</td>
</tr>
<tr>
<td>Primary DNS: 172.19.1.1 (DHCP)</td>
</tr>
<tr>
<td>Secondary DNS: 172.19.1.2 (DHCP)</td>
</tr>
</tbody>
</table>

**Cache Entries**

There are no entries in the cache.

[Remove All]
**To find a DNS Name or IP Address:**

1. Enter either a DNS name or an IP address.
2. Click **Lookup**.
   - When a DNS name is resolved, the results appear in the DNS cache.
   - When an IP address is resolved, the results appear in a text below the Lookup field.

**To clear cache entries:**

1. Click **Remove All** to remove all listed cache entries.
2. Click **Delete** next to a specific cache entry to remove only that one.

---

**Point-to-Point (PPP) Settings**

Point-to-Point Protocol 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 device server 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. The MatchPort AR embedded device server also supports the authentication scheme of “None” when no authentication is required during link negotiation.

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 embedded device server also supports authentication scheme of “None” when no authentication is required during link negotiation.

Since the MatchPort AR unit 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 device 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.

**Note:** *The MatchPort AR embedded device server 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 unit, 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 network interface IP
Address of the MatchPort AR embedded device server as its gateway.

The following section describes the steps to configure PPP 1 (PPP on serial line 1); these steps
also apply to any line instance of the device. Since the MatchPort AR unit does not support NAPT
(Network Address and Port Translation), static routing table entries must be added to both the
serial-side and network-side devices (both of which are external to the MatchPort AR embedded
device server).

To configure PPP:
1. Select PPP on the menu bar. The PPP web page appears.
2. Select a line number at the top of the page. The PPP Configuration page for the selected line
   number appears.

3. Enter or modify the following settings:

   **Table 9-3 PPP Configuration**

<table>
<thead>
<tr>
<th>PPP Configuration Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local IP Address</td>
<td>Enter the IP address assigned to the device’s PPP interface.</td>
</tr>
<tr>
<td>Peer IP Address</td>
<td>Enter the IP address assigned to the peer (when requested during negotiation).</td>
</tr>
</tbody>
</table>

   **Figure 9-2 PPP Configuration Settings**

   ![PPP Configuration Settings](image)
4. Click **Submit**.

5. Repeat above steps as desired, according to additional line(s) available on your product.

### SNMP Settings

Simple Network Management Protocol (SNMP) is a network management tool that monitors network devices for conditions that need attention. The SNMP service responds to SNMP requests and generates SNMP Traps.

This page is used to configure the SNMP agent.

**To configure SNMP:**

1. Select **SNMP** on the menu bar. The SNMP page opens and shows the current SNMP configuration.

   **Figure 9-4  SNMP Configuration**

<table>
<thead>
<tr>
<th>SNMP</th>
</tr>
</thead>
<tbody>
<tr>
<td>State: Enabled</td>
</tr>
<tr>
<td>Read Community:</td>
</tr>
<tr>
<td>Write Community:</td>
</tr>
<tr>
<td>System Contact:</td>
</tr>
<tr>
<td>System Name:</td>
</tr>
<tr>
<td>System Description:</td>
</tr>
<tr>
<td>System Location:</td>
</tr>
<tr>
<td>Traps State: Enabled</td>
</tr>
<tr>
<td>Traps Primary Destination:</td>
</tr>
<tr>
<td>Traps Secondary Destination:</td>
</tr>
</tbody>
</table>

**Note:** The system description string will reflect the specific Lantronix product.
2. Enter or modify the following settings:

<table>
<thead>
<tr>
<th>SNMP Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>Select <strong>Enabled</strong> to enable SNMP.</td>
</tr>
<tr>
<td>Read Community</td>
<td>Enter the SNMP read-only community string.</td>
</tr>
<tr>
<td>Write Community</td>
<td>Enter the SNMP read/write community string.</td>
</tr>
<tr>
<td>System Contact</td>
<td>Enter the name of the system contact.</td>
</tr>
<tr>
<td>System Name</td>
<td>Enter the system name.</td>
</tr>
<tr>
<td>System Description</td>
<td>Enter the system description.</td>
</tr>
<tr>
<td>System Location</td>
<td>Enter the system location.</td>
</tr>
<tr>
<td>Traps State</td>
<td>Select <strong>Enabled</strong> to enable the transmission of SNMP Traps. The Cold Start trap is sent on device boot up, and the Linkdown trap is sent when the device is rebooted from software control.</td>
</tr>
<tr>
<td>Traps Primary Destination</td>
<td>Enter the primary SNMP trap host.</td>
</tr>
<tr>
<td>Traps Secondary Destination</td>
<td>Enter the secondary SNMP trap host.</td>
</tr>
</tbody>
</table>

3. Click **Submit**.
FTP Settings

The FTP web page shows the current File Transfer Protocol (FTP) configuration and various statistics about the FTP server.

To configure FTP:

1. Select FTP on the menu bar. The FTP page opens to display the current configuration.

![Figure 9-6 FTP Configuration](image)

2. Enter or modify the following settings:

<table>
<thead>
<tr>
<th>FTP Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>Select <strong>Enabled</strong> to enable the FTP server.</td>
</tr>
<tr>
<td>Admin Username</td>
<td>Enter the username to use when logging in via FTP.</td>
</tr>
<tr>
<td>Admin Password</td>
<td>Enter the password to use when logging in via FTP.</td>
</tr>
</tbody>
</table>

3. Click **Submit**.

---

**MatchPort® AR Embedded Device Server User Guide**
TFTP Settings

In the TFTP web page, you can configure the server and view the statistics about the Trivial File Transfer Protocol (TFTP) server.

**To configure TFTP:**

1. Select **TFTP** on the menu bar. The TFTP page opens to display the current configuration.

2. Enter or modify the following settings:

   **Table 9-9 TFTP Server**

<table>
<thead>
<tr>
<th>TFTP Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>Select <strong>Enabled</strong> to enable the TFTP server.</td>
</tr>
<tr>
<td>Allow TFTP File Creation</td>
<td>Select whether to allow the creation of new files stored on the TFTP server.</td>
</tr>
</tbody>
</table>
   | 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 update. |
   | Allow XCR Import        | Specifies whether the TFTP server is allowed to accept an XML configuration file for update. An attempt to import configuration is recognized based on the name of the file.  
   |                          | **Note:** TFTP cannot authenticate the client, so the device is open to malicious update. |

3. Click **Submit**.
Syslog Settings

The Syslog web page shows the current configuration and statistics of the system log. Here you may configure the syslog destination and the severity of the events to log.

To configure the Syslog:

**Note:** The syslog file is always saved to local storage, but it is not retained through 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. Select **Syslog** on the menu bar. The Syslog page opens to display the current configuration.

![Figure 9-10 Syslog](image)

2. Enter or modify the following settings:

   ![Table 9-11 Syslog](image)

   **Table 9-11 Syslog**

<table>
<thead>
<tr>
<th>Syslog Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>Select to enable or disable the syslog.</td>
</tr>
<tr>
<td>Host</td>
<td>Enter the IP address of the remote server to which system logs are sent for storage.</td>
</tr>
<tr>
<td>Local Port</td>
<td>Enter the number of the local port on the device from which system logs are sent.</td>
</tr>
<tr>
<td>Remote Port</td>
<td>Enter the number of the port on the remote server that supports logging services. The default is 514.</td>
</tr>
<tr>
<td>Severity Log Level</td>
<td>From the drop-down box, select the minimum level of system message the device should log. This setting applies to all syslog facilities. The drop-down list is in descending order of severity (e.g., <strong>Emergency</strong> is more severe than <strong>Alert</strong>.)</td>
</tr>
</tbody>
</table>

3. Click **Submit**.
HTTP Settings

Hypertext Transfer Protocol (HTTP) is the transport protocol for communicating hypertext documents on the Internet. HTTP defines how messages are 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.

This page has three links at the top for viewing statistics and for viewing and changing configuration and authentication settings.

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

HTTP Statistics

To view HTTP statistics:

This page shows various statistics about the HTTP server.

1. Select HTTP on the menu bar and then Statistics at the top of the page. The HTTP Statistics page appears.

![Figure 9-12 HTTP Statistics](image)

<table>
<thead>
<tr>
<th>HTTP Statistics</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Rx Bytes</td>
<td>26256</td>
</tr>
<tr>
<td>Tx Bytes</td>
<td>198244</td>
</tr>
<tr>
<td>200 - OK</td>
<td>15</td>
</tr>
<tr>
<td>301 - Moved Permanently</td>
<td>0</td>
</tr>
<tr>
<td>400 - Bad Request</td>
<td>0</td>
</tr>
<tr>
<td>401 - Authorization Required</td>
<td>13</td>
</tr>
<tr>
<td>404 - Not Found</td>
<td>0</td>
</tr>
<tr>
<td>408 - Request Timeout</td>
<td>0</td>
</tr>
<tr>
<td>413 - Request Too Large</td>
<td>0</td>
</tr>
<tr>
<td>500 - Internal Error</td>
<td>0</td>
</tr>
<tr>
<td>501 - Not Implemented</td>
<td>0</td>
</tr>
<tr>
<td>Status Unknown</td>
<td>0</td>
</tr>
<tr>
<td>Work Queue Full</td>
<td>0</td>
</tr>
<tr>
<td>Socket Error</td>
<td>0</td>
</tr>
<tr>
<td>Memory Error</td>
<td>0</td>
</tr>
<tr>
<td>Logs</td>
<td>42 entries</td>
</tr>
</tbody>
</table>

*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 Page.
HTTP Configuration

On this page you may change HTTP configuration settings.

To configure HTTP:

1. Select HTTP on the menu bar and then Configuration at the top of the page. The HTTP Configuration page opens.

Figure 9-13 HTTP Configuration

2. Enter or modify the following settings:

Table 9-14 HTTP Configuration

<table>
<thead>
<tr>
<th>HTTP Configuration Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>Select Enabled to enable the HTTP server.</td>
</tr>
<tr>
<td>Port</td>
<td>Enter the port for the HTTP server to use. The default is 80.</td>
</tr>
<tr>
<td>Secure Port</td>
<td>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.</td>
</tr>
</tbody>
</table>
3. Click Submit.
HTTP Authentication

HTTP Authentication enables you to require usernames and passwords to access specific web pages or directories on the MatchPort AR® built-in web server.

To configure HTTP authentication settings:

1. Select HTTP on the menu bar and then Authentication at the top of the page. The HTTP Authentication page opens.

2. Enter or modify the following settings:

   Table 9-16 HTTP Authentication

   Note: To properly view data entries in RSS Settings in certain web browsers, it may be necessary to first remove authentication from RSS. Enter the following under HTTP Authentication: URI: “/rss”, Realm: “rss”, and AuthType: “None”.

<table>
<thead>
<tr>
<th>HTTP Authentication Settings</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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. |
HTTP Authentication Settings (continued) | 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. 
*Note:* When changing the parameters of Digest or SSL Digest authentication, it is often best to close and reopen the browser to ensure it does not attempt to use cached authentication information.

**Username** | Enter the **Username** used to access the **URI**. More than one Username per URI is permitted. 
Click **Submit** and enter the next Username as necessary.

**Password** | Enter the **Password** for the **Username**.

3. Click **Submit**.

4. To delete the URI and users, click **Delete** in the current configuration table.

*Note:* The **URI**, realm, **username**, and **password** are user-specified, free-form fields. The **URI** must match the directory created on the MatchPort AR file system.
RSS Settings

Really Simple Syndication (RSS) (sometimes referred to as Rich Site Summary) is a method of feeding online content to Web users. Instead of actively searching for MatchPort AR configuration changes, RSS feeds permit viewing only relevant and new information regarding changes made to the MatchPort AR embedded device server via an RSS publisher. The RSS feeds may also be stored to the file system cfg_log.txt file.

To configure RSS settings:

1. Select RSS on the menu bar. The RSS page opens and shows the current RSS configuration.

![Figure 9-17 RSS](image)

2. Enter or modify the following settings:

![Table 9-18 RSS](table)

3. Select Submit.

4. In the Current Status table, view and clear stored RSS Feed entries, as necessary.
LPD Settings

The MatchPort AR device acts as a print server if a printer gets connected to one of its serial ports. Selecting 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

This read-only page shows various statistics about the LPD server.

To view LPD statistics for a specific LPD line:

1. Select LPD on the menu bar. The LPD web page appears. Select an LPD line at the top of the page. Select Statistics. The LPD Statistics page for the selected LPD line appears. Repeat above steps as desired, according to additional LPD(s) available on your product.

Figure 9-19 LPD Statistics

<table>
<thead>
<tr>
<th>LPD 1</th>
<th>LPD 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Statistics</td>
<td>Configuration</td>
</tr>
</tbody>
</table>

LPD 1 - Statistics

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

Here you can change LPD configuration settings.

To configure LPD settings for a specific LPD line:

1. Select LPD on the menu bar, if you are not already at the LPD web page. Select a LPD line at the top of the page. Select Configuration. The LPD Configuration for the selected LPD line appears.

Figure 9-20 LPD Configuration

<table>
<thead>
<tr>
<th>LPD 1</th>
<th>LPD 2</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Statistics</td>
<td>Configuration</td>
</tr>
</tbody>
</table>

**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:**

2. Enter or modify the following settings:

Table 9-21 LPD Configuration

<table>
<thead>
<tr>
<th>LPD Configuration Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Banner</strong></td>
<td>Select Enabled to print the banner even if the print job does not specify to do so. Selected by default.</td>
</tr>
<tr>
<td><strong>Binary</strong></td>
<td>Select Enabled for the device to pass the entire file to the printer unchanged. Otherwise, the device 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.</td>
</tr>
<tr>
<td><strong>Start of Job</strong></td>
<td>Select Enabled to print a &quot;start of job&quot; string before sending the print data.</td>
</tr>
<tr>
<td><strong>End of Job</strong></td>
<td>Select Enabled to send an &quot;end of job&quot; string.</td>
</tr>
</tbody>
</table>
9: Service Settings

<table>
<thead>
<tr>
<th>LPD Configuration Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Formfeed</td>
<td>Select Enabled to force the printer to advance to the next page at the end of each print job.</td>
</tr>
<tr>
<td>Convert Newlines</td>
<td>Select Enabled to convert single newlines and carriage returns to DOS-style line endings.</td>
</tr>
<tr>
<td>SOJ String</td>
<td>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.</td>
</tr>
<tr>
<td>EOJ String</td>
<td>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.</td>
</tr>
<tr>
<td>Queue Name</td>
<td>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)</td>
</tr>
</tbody>
</table>

3. Click Submit. Repeat above steps as desired, according to additional LPD lines available on your product.
10: Security Settings

The MatchPort AR embedded device server 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 device server 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 Cipher Suites
- SSL Certificates
- SSL RSA or DSA
- SSL Certificates and Private Keys
- SSL Utilities
- SSL Configuration

Note: For more information, see Chapter 14: Security in Detail on page 137.

SSH Settings

SSH is a network protocol for securely accessing a remote device over an encrypted channel. This protocol manages the security of internet data transmission between two hosts over a network by providing encryption, authentication, and message integrity services.

Two instances require configuration: when the MatchPort AR unit is the SSH server and when it is an SSH client. The SSH server is used by the CLI (Command Mode) and for tunneling in Accept Mode. The SSH client is for tunneling in Connect Mode.

To configure the MatchPort AR embedded device server as an SSH server, there are two requirements:

- Defined Host Keys: both private and public keys are required. These keys are used for the Diffie-Hellman key exchange (used for the underlying encryption protocol).
- Defined Users: these users are permitted to connect to the MatchPort AR SSH server.
This page has four links at the top for viewing and changing SSH server host keys, SSH server authorized keys, SSH client known hosts, and SSH client users.

**SSH Server Host Keys**

SSH Host Keys can be obtained in a few different ways:

- Uploading keys via PUTTY or other tools which generate RFC4716 format keys.
- Creating keys through the device.

The steps for creating or uploading keys is described below.

**To upload SSH server host keys generated from PuTTY:**

1. Create the keys with puttygen.exe. The keys are in PuTTY format.
2. Use puttygen.exe again to convert the private key to Open SSH format as follows:
   a. Import the private key using "Conversions...Import key."
   b. Create a new file using "Conversions...Export OpenSSH key."
3. Use ssh-keygen to convert the public key to OpenSSH format.
   
   `ssh-keygen -i -f putty_file > openssh_file`
4. Select SSH on the menu bar and **SSH Server: Host Keys** at the top of the page. The SSH Server Host Keys page appears.

![SSH Server: Host Keys (Upload Keys)](image)
5. Enter or modify the following settings in the part of the screen related to uploading keys:

<table>
<thead>
<tr>
<th>SSH Server: Host Keys Settings (continued)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Private Key</strong></td>
<td>Enter the path and name of the existing private key you want to upload or use the <strong>Browse</strong> 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.</td>
</tr>
<tr>
<td><strong>Public Key</strong></td>
<td>Enter the path and name of the existing public key you want to upload or use the <strong>Browse</strong> button to select the key.</td>
</tr>
</tbody>
</table>
| **Key Type**                             | Select a key type to use for the new key:  
  - **RSA** = use this key with the SSH1 and SSH2 protocols.  
  - **DSA** = use this key with the SSH2 protocol. |

6. Click **Submit**.

*To upload SSH server host RFC4716 format keys:*

1. Use any program that can produce keys in the RFC4716 format.
2. Use ssh-keygen to convert the format to OpenSSH.
   ```bash
   ssh-keygen -i -f RFC4716_file > output_file
   ```

*Note:* If the keys do not exist, follow directions under **To create new SSH server host keys** (on page 87).

3. Select **SSH** on the menu bar and **SSH Server: Host Keys** at the top of the page. The SSH Server Host Keys page appears.
4. Enter or modify the following settings in the part of the screen related to uploading keys:

Table 10-4  SSH Server Host Keys Settings - Upload Keys Method

<table>
<thead>
<tr>
<th>SSH Server: Host Keys Settings (continued)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Private Key</strong></td>
<td>Enter the path and name of the existing private key you want to upload or use the <strong>Browse</strong> 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.</td>
</tr>
<tr>
<td><strong>Public Key</strong></td>
<td>Enter the path and name of the existing public key you want to upload or use the <strong>Browse</strong> button to select the key.</td>
</tr>
</tbody>
</table>
| **Key Type**                             | Select a key type to use for the new key:  
  - **RSA** = use this key with the SSH1 and SSH2 protocols.  
  - **DSA** = use this key with the SSH2 protocol. |

5. Click **Submit**.

*Note: SSH keys may be created on another computer and uploaded to the MatchPort AR embedded device server. For example, use the following command using Open SSH to create a 1024-bit DSA key pair: `ssh-keygen -b 1024 -t dsa`
To create new SSH server host keys

**Note:** Generating new keys with large bit size results in longer key generation times.

1. Select SSH on the menu bar and **SSH Server: Host Keys** at the top of the page. The SSH Server Host Keys page appears.

   ![SSH Server: Host Keys (Create New Keys)](image)

   **Figure 10-5  SSH Server: Host Keys (Create New Keys)**

2. Enter or modify the following settings in the part of the screen related to creating new keys:

   **Table 10-6  SSH Server Host Keys Settings - Create New Keys Method**

<table>
<thead>
<tr>
<th>SSH Server: Host Keys Settings</th>
<th>Description</th>
</tr>
</thead>
</table>
   | 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.  
   | **Note:** RSA is more secure.    |             |
3. Click **Submit**.

**Note:** SSH Keys from other programs may be converted to the required MatchPort AR format. Use Open SSH to perform the conversion.

### SSH Server Authorized Users

On this page you can change SSH server settings for Authorized Users. SSH Server Authorized Users are accounts on the MatchPort AR embedded device server that can be used to log into the using SSH. For instance, these accounts can be used to SSH into the CLI or open an SSH connection to a device port. Every account must have a password.

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

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

**To configure the SSH server for authorized users:**

1. Select **SSH** on the menu bar and then **Server Authorized Users** at the top of the page. The SSH Server: Authorized Users page appears.
2. Enter or modify the following settings:

**Table 10-8 SSH Server Authorized User Settings**

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

3. Click **Submit**.

**Note:** When uploading the security keys, ensure the keys are not compromised in transit.
SSH Client Known Hosts

On this page you can change SSH client settings for known hosts.

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

**To configure the SSH client for known hosts:**

1. Select SSH on the menu bar and then **Client Known Hosts** at the top of the page. The SSH Client: Known Hosts page appears.

2. Enter or modify the following settings:

   **Table 10-10  SSH Client Known Hosts**

<table>
<thead>
<tr>
<th>SSH Client: Known Hosts Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Server</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Public RSA Key</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Public DSA Key</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>

   **Note:** These settings are not required for communication. They protect against Man-In-The-Middle (MITM) attacks.

3. Click **Submit**.

4. In the **Current Configuration** table, delete currently stored settings as necessary.
SSH Client Users

On this page you can change SSH client settings for users. To configure the MatchPort AR embedded device server as an SSH client, an SSH client user must be both configured and also exist on the remote SSH server.

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

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

To configure the SSH client users:

1. Select SSH on the menu bar and then SSH Client Users at the top of the page. The SSH Client: Users page appears.

![Figure 10-11  SSH Client: Users](image)
2. Enter or modify the following settings:

<table>
<thead>
<tr>
<th>SSH Client: Users Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>Enter the name that the device uses to connect to a SSH server.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password associated with the username.</td>
</tr>
<tr>
<td>Remote Command</td>
<td>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.</td>
</tr>
<tr>
<td>Private Key</td>
<td>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.</td>
</tr>
<tr>
<td>Public Key</td>
<td>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.</td>
</tr>
</tbody>
</table>

*Note:* If the user public key is known on the remote SSH server, the SSH server does not require a password. The Remote Command is provided to the SSH server upon connection. It specifies the application to execute upon connection. The default is a command shell.

*Note:* Configuring the SSH client’s known hosts is optional. It prevents Man-In-The-Middle (MITM) attacks.

<table>
<thead>
<tr>
<th>Key Type</th>
<th>Select the key type to be used. Choices are:</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSA</td>
<td>use this key with the SSH1 and SSH2 protocols.</td>
</tr>
<tr>
<td>DSA</td>
<td>use this key with the SSH2 protocol.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Create New Keys</th>
<th>Username</th>
<th>Enter the name of the user associated with the new key.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key Type</td>
<td>Select the key type to be used for the new key. Choices are:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>RSA</td>
<td>use this key with the SSH1 and SSH2 protocols.</td>
</tr>
<tr>
<td></td>
<td>DSA</td>
<td>use this key with the SSH2 protocol.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Bit Size</th>
<th>Select the bit length of the new key:</th>
</tr>
</thead>
<tbody>
<tr>
<td>512</td>
<td></td>
</tr>
<tr>
<td>768</td>
<td></td>
</tr>
<tr>
<td>1024</td>
<td></td>
</tr>
</tbody>
</table>

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. This device 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.
4. In the Current Configuration table, delete currently stored settings as necessary.
SSL Settings

Secure Sockets Layer (SSL) is a protocol for managing the security of data transmission over the Internet. It provides encryption, authentication, and message integrity services. SSL is widely used for secure communication to a web server.

Certificate/Private key combinations can be obtained from an external Certificate Authority (CA) and downloaded into the unit. Self-signed certificates with associated private key can be generated by the device server itself.

For more information regarding Certificates and how to obtain them, see SSL Certificates and Private Keys (on page 94).

SSL uses digital certificates for authentication and cryptography against eavesdropping and tampering. Sometimes only the server is authenticated; sometimes both server and client are authenticated. The AR embedded device server can be server and/or client, depending on the application. Public key encryption systems exchange information and keys and set up the encrypted tunnel.

Efficient symmetric encryption methods encrypt the data going through the tunnel after it is established. Hashing provides tamper detection.

Applications that can make use of SSL are Tunneling, Secure Web Server, and WLAN interface.

The MatchPort AR unit supports SSLv3 and its successors, TLS1.0 and TLS1.1.

Note: An incoming SSLv2 connection attempt is answered with an SSLv3 response. If the initiator also supports SSLv3, SSLv3 handles the rest of the connection.

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. Supported cipher suites include the following:

<table>
<thead>
<tr>
<th>Certificate</th>
<th>Key Exchange</th>
<th>Encryption</th>
<th>Hash</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSA</td>
<td>DHE</td>
<td>3DES</td>
<td>SHA1</td>
</tr>
<tr>
<td>RSA</td>
<td>RSA</td>
<td>128 bits AES</td>
<td>SHA1</td>
</tr>
<tr>
<td>RSA</td>
<td>RSA</td>
<td>Triple DES</td>
<td>SHA1</td>
</tr>
<tr>
<td>RSA</td>
<td>RSA</td>
<td>128 bits RC4</td>
<td>MD5</td>
</tr>
<tr>
<td>RSA</td>
<td>RSA</td>
<td>128 bits RC4</td>
<td>SHA1</td>
</tr>
<tr>
<td>RSA</td>
<td>1024 bits RSA</td>
<td>56 bits RC4</td>
<td>MD5</td>
</tr>
<tr>
<td>RSA</td>
<td>1024 bits RSA</td>
<td>56 bits RC4</td>
<td>SHA1</td>
</tr>
<tr>
<td>RSA</td>
<td>1024 bits RSA</td>
<td>40 bits RC4</td>
<td>MD5</td>
</tr>
</tbody>
</table>

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 require 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 other 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 and/or SSL Tunneling in Accept mode, the MatchPort AR unit needs a personal certificate with a matching private key to identify itself and sign its messages. When using SSL Tunneling in Connect mode, the MatchPort AR embedded device server 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 embedded device server 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 unit, 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 you can generate your own. A few utilities exist to generate self-signed certificates or sign certificate requests. The MatchPort AR embedded device server 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 unit.

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 embedded device server currently only accepts separate PEM files. The key needs to be unencrypted.
SSL Utilities
Several utilities exist to convert between the formats.

OpenSSL
Open source is a 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:

```bash
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.
SSL Configuration

To configure SSL settings:

1. Select SSL from the main menu. The SSL page appears.

![SSL Configuration Page]

**Figure 10-14 SSL**
2. Enter or modify the following settings:

**Table 10-15 SSL**

<table>
<thead>
<tr>
<th>SSL Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Upload Certificate</td>
<td><strong>New Certificate</strong>&lt;br&gt;Enter the path and name of the certificate you want to upload, or use the <strong>Browse</strong> button to select the certificate. RSA or DSA certificates with 512 to 1024 bit public keys are allowed.&lt;br&gt;The format of the file must be <strong>PEM</strong>. The file must start with &quot;-----BEGIN CERTIFICATE-----&quot; and end with &quot;-----END CERTIFICATE-----&quot;. Some Certificate Authorities add comments before and/or after these lines. Those need to be deleted before upload.</td>
</tr>
<tr>
<td></td>
<td><strong>New Private Key</strong>&lt;br&gt;Enter the path and name of the private key you want to upload, or use the <strong>Browse</strong> button to select the private key. The key needs to belong to the certificate entered above.&lt;br&gt;The format of the file must be <strong>PEM</strong>. The file must start with &quot;-----BEGIN RSA PRIVATE KEY-----&quot; and end with &quot;-----END RSA PRIVATE KEY-----&quot;. Read <strong>DSA</strong> instead of <strong>RSA</strong> in case of a <strong>DSA</strong> key. Some Certificate Authorities add comments before and/or after these lines. Those need to be deleted before upload.</td>
</tr>
<tr>
<td></td>
<td><strong>Upload Authority Certificate</strong>&lt;br&gt;<strong>Authority</strong>&lt;br&gt;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.&lt;br&gt;Enter the path and name of the certificate you want to upload, or use the <strong>Browse</strong> button to select the certificate. RSA or DSA certificates with 512 to 1024 bit public keys are allowed.&lt;br&gt;The format of the file must be <strong>PEM</strong>. The file must start with &quot;-----BEGIN CERTIFICATE-----&quot; and end with &quot;-----END CERTIFICATE-----&quot;. Some Certificate Authorities add comments before and/or after these lines. Those need to be deleted before upload.</td>
</tr>
<tr>
<td></td>
<td><strong>Create New Self-Signed Certificate</strong>&lt;br&gt;<strong>Country (2 Letter Code)</strong>&lt;br&gt;Enter the 2-letter country code to be assigned to the new self-signed certificate.&lt;br&gt;<strong>Examples</strong>: US for United States and CA for Canada&lt;br&gt;<strong>State/Province</strong>&lt;br&gt;Enter the state or province to be assigned to the new self-signed certificate. <strong>Locality (City)</strong>&lt;br&gt;Enter the city or locality to be assigned to the new self-signed certificate. <strong>Organization</strong>&lt;br&gt;Enter the organization to be associated with the new self-signed certificate.&lt;br&gt;<strong>Example</strong>: If your company is called Widgets, and you are setting up a web server for the Sales department, enter Widgets for the organization. <strong>Organization Unit</strong>&lt;br&gt;Enter the organizational unit to be associated with the new self-signed certificate.&lt;br&gt;<strong>Example</strong>: If your company is setting up a web server for the Sales department, enter Sales for your organizational unit.</td>
</tr>
</tbody>
</table>
### SSL Settings (continued)

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Common Name</strong></td>
</tr>
<tr>
<td>Enter the same name that the user will enter when requesting your web site. Example: If a user enters <a href="http://www.widgets.abccompany.com">http://www.widgets.abccompany.com</a> to access your web site, the <strong>Common Name</strong> would be <a href="http://www.widgets.abccompany.com">www.widgets.abccompany.com</a>.</td>
</tr>
</tbody>
</table>

| **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. |

| **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. |

3. Click **Submit**. 
11: Modbus

Modbus ASCII/RTU based serial slave devices can be connected via the ethernet through an existing Modbus TCP/IP network. Any device having access to a given Modbus implementation will be able to perform full range of operations that the implementation supports. Modbus/TCP uses a reserved TCP port of 502 and include a single byte function code (1=255) preceded by a 6 byte header:

**Table 11-1 6 Byte Header of Modbus Application Protocol**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transaction ID</td>
<td>Identification of request/response transaction - copied by slave</td>
</tr>
<tr>
<td>Protocol ID</td>
<td>0 - Modbus protocol</td>
</tr>
<tr>
<td>Length</td>
<td>Number of following bytes includes the unit identifier</td>
</tr>
<tr>
<td>Address</td>
<td>Identification of remove slave</td>
</tr>
</tbody>
</table>

**CP Control via Modbus**

Default groups are mapped to Modbus registers. CPs added to groups will result in the CP being read and written based on the reading or writing to the register which maps to that CP group. Default Modbus group names include:

- Modbus_Ctl_In
- Modbus_Ctl_Out

**Note:** Refer to Chapter 8: CPM: Groups on page 62 for instructions on adding a CP to a Group.

When the Modbus slave address is set to 0xFF, the message is addressed to the internal default groups and thus processed by the MatchPort AR embedded device server. The Modbus 'local slave' supported functions are listed in the table below.

**Table 11-2 Modbus Local Slave Functions - Query**

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Read Coils</td>
<td>0x01</td>
<td>0x00</td>
<td>0x00-0x02</td>
<td>0x00</td>
<td>0x01-0x03</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Starting CP CP 1 – CP 3</td>
<td></td>
<td>No of CPs to output</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Read Input status</td>
<td>0x02</td>
<td>0x00</td>
<td>0x00-0x02</td>
<td>0x00</td>
<td>0x01-0x03</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Starting CP CP 1 – CP 3</td>
<td></td>
<td>No of CPs to output</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Read Holding Registers</td>
<td>0x03</td>
<td>0x00</td>
<td>0x00-0x02</td>
<td>0x00</td>
<td>0x01-0x03</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Starting CP CP 1 – CP 3</td>
<td></td>
<td>No of CPs to output</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Read Input Registers</td>
<td>0x04</td>
<td>0x00</td>
<td>0x00-0x02</td>
<td>0x00</td>
<td>0x01-0x03</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Starting CP CP 1 – CP 3</td>
<td></td>
<td>No of CPs to output</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-----------------------------</td>
<td>--------</td>
<td>----------------</td>
<td>----------------</td>
<td>-------------</td>
<td>-------------</td>
<td>----------------</td>
<td>-----------</td>
</tr>
<tr>
<td>Force Single Coil</td>
<td>0x05</td>
<td>0x00</td>
<td>0x00-0x02</td>
<td>0x00-0x02</td>
<td>0xff (set CPx to 1) or 0x00 (set CPx to 0)</td>
<td>0x00</td>
<td>N/A</td>
</tr>
<tr>
<td>Preset Single Register</td>
<td>0x06</td>
<td>0x00</td>
<td>0x00-0x02</td>
<td>0x00</td>
<td>0x00</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Force Multiple Coils</td>
<td>0x0F</td>
<td>0x00</td>
<td>0x00-0x02</td>
<td>0x00</td>
<td>0x01-0x03 No of CPs to set</td>
<td>0x01</td>
<td>0B00000xyz CP values _Lo CP# in low bit</td>
</tr>
<tr>
<td>Preset Multiple Registers</td>
<td>0x10</td>
<td>0x00</td>
<td>0x00-0x02</td>
<td>0x00</td>
<td>0x01-0x03 No of CPs to set</td>
<td>0x02-0x06 No of CPs to set * 2</td>
<td>Max [6]. 0x00, 0x0Y 0x00, 0x0Y Y = 0 or 1</td>
</tr>
<tr>
<td>Read/Write 4X Registers</td>
<td>0x17</td>
<td>0x00</td>
<td>0x00-0x02</td>
<td>0x00</td>
<td>0x01-0x03 Quantity to read</td>
<td>0x00</td>
<td>0x00-0x02 Starting CP CP1 – CP3 to write</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0x00-0x03 Quantity to write</td>
<td>0x02-0x06 (Quantity to write) * 2</td>
<td>Max [6]. 0x00, 0x0Y 0x00, 0x0Y Y = 0 or 1</td>
<td></td>
</tr>
</tbody>
</table>

### Table 11-3 Modbus Local Slave Functions - Response

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Read Coils</td>
<td>0x01</td>
<td>0x01</td>
<td>0B00000xyz CP output values _Lo CP# in high bit</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Read Input status</td>
<td>0x02</td>
<td>0x01</td>
<td>0B00000xyz CP output values _Lo CP# in high bit</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Read Holding Registers</td>
<td>0x03</td>
<td>0x02-0x06</td>
<td>0x00</td>
<td>Starting CP Value 0x00 or 0x01</td>
<td>0x00</td>
<td>Next CP or End CP value 0x00 or 0x01</td>
<td>0x00</td>
<td>End CP value 0x00 or 0x01</td>
</tr>
<tr>
<td>Read Input Registers</td>
<td>0x04</td>
<td>0x02-0x06</td>
<td>0x00</td>
<td>Starting CP Value 0x00 or 0x01</td>
<td>0x00</td>
<td>Next CP or End CP value 0x00 or 0x01</td>
<td>0x00</td>
<td>End CP value 0x00 or 0x01</td>
</tr>
<tr>
<td>Force Single Cell</td>
<td>0x05</td>
<td>Echo query</td>
<td>Echo query</td>
<td>Echo query</td>
<td>Echo query</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Preset Single Register</td>
<td>0x06</td>
<td>Echo query</td>
<td>Echo query</td>
<td>Echo query</td>
<td>Echo query</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>
Evolution OS® products can be set up to communicate on standard Modbus networks using either RTU or ASCII. Users select the desired mode and serial port communication parameters (baud rate, parity mode, etc) when in the line configuration options.

**Table 11-4 Modbus Transmission Modes**

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Force Multiple Coil</td>
<td>0x0F</td>
<td>Echo query</td>
<td>Echo query</td>
<td>Echo query</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Preset Multiple Registers</td>
<td>0x10</td>
<td>Echo query</td>
<td>Echo query</td>
<td>Echo query</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Read/Write 4X Registers</td>
<td>0x17</td>
<td>0x02-0x06 (Quantity of Read) * 2</td>
<td>Max [6]. 0x00, 0x01Y 0x00, 0x01Y 0x00, 0x01Y Y = 0 or 1</td>
<td>Echo query</td>
<td>N/A</td>
<td>N/A</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The Modbus web pages allow you to check Modbus status and make configuration changes. This chapter contains the following sections:

- *Modbus Statistics*
- *Modbus Configuration*
Modbus Statistics

This read-only web page displays the current connection status of the Modbus servers listening on the TCP ports. When a connection is active, the remote client information is displayed as well as the number of PDUs that have been sent and received. Additionally, a Kill link will be present which can be used to kill the connection.

To view modbus statistics:

1. Click Modbus on the menu bar and click Statistics at the top of the page. The Modbus Statistics page appears.

Figure 11-5 Modbus Statistics

<table>
<thead>
<tr>
<th>TCP Server</th>
<th>Statistics</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>State:</td>
<td>Up</td>
<td></td>
</tr>
<tr>
<td>Port:</td>
<td>502</td>
<td></td>
</tr>
<tr>
<td>Last Connection:</td>
<td>local 502 &lt;-&gt; 172.19.205.10:3903</td>
<td></td>
</tr>
<tr>
<td>Uptime:</td>
<td>0 days 02:36:20</td>
<td></td>
</tr>
<tr>
<td>Total PDUs In:</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Total PDUs Out:</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Total Connections:</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Current Connections:</td>
<td>local 502 &lt;-&gt; 172.19.205.10:3903 [Kill]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Uptime: 0 days 02:36:48</td>
<td></td>
</tr>
<tr>
<td></td>
<td>PDUs In: 0</td>
<td></td>
</tr>
<tr>
<td></td>
<td>PDUs Out: 0</td>
<td></td>
</tr>
<tr>
<td>Additional TCP Server</td>
<td></td>
<td></td>
</tr>
<tr>
<td>State:</td>
<td>Up</td>
<td></td>
</tr>
<tr>
<td>Port:</td>
<td>505</td>
<td></td>
</tr>
<tr>
<td>Last Connection:</td>
<td>&lt;None&gt;</td>
<td></td>
</tr>
<tr>
<td>Uptime:</td>
<td>0 days 02:35:53</td>
<td></td>
</tr>
<tr>
<td>Total PDUs In:</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Total PDUs Out:</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Total Connections:</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Current Connections:</td>
<td>&lt;None&gt;</td>
<td></td>
</tr>
<tr>
<td>Local Slave</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total PDUs In:</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Total PDUs Out:</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Exception Count:</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>
Modbus Configuration

This web page shows the current negotiated Modbus settings and allows configuration changes.

To view and configure the Modbus Server:

1. Click **Modbus** on the menu bar and then click **Configuration** at the top of the page. The Modbus Configuration page appears.

2. Enter or modify the following settings:

   **Table 11-7  Modbus Configuration**

<table>
<thead>
<tr>
<th>Modbus Configuration Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP Server State</td>
<td>If On, the Modbus server is active on TCP 502.</td>
</tr>
<tr>
<td>Additional TCP Server Port</td>
<td>If present, is used in addition to TCP port 502.</td>
</tr>
<tr>
<td>Response Timeout</td>
<td>The number of milliseconds to wait for a response on the serial side. The device returns exception code 11 to the network master controller if the slave serial device fails to reply within this time out.</td>
</tr>
<tr>
<td>RSS Trace Input</td>
<td>If On, each PDU received on the Modbus serial line creates a non-persistent descriptive item in the RSS feed.</td>
</tr>
</tbody>
</table>

3. Click **Submit**. The changes take effect immediately.

**Note:** The serial line protocol must also be configured for Modbus, in addition to configuring the Modbus server. See **Chapter 6: Line and Tunnel Settings on page 33** for details.
12: Maintenance and Diagnostics Settings

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

- Filesystem Settings
- Protocol Stack Settings
- IP Address Filter
- Query Port
- Diagnostics
- System Settings

Filesystem Settings

The embedded device server uses a flash filesystem to store files. Use the Filesystem option to view current file statistics or modify files. There are two subsections: Statistics and Browse.

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

Filesystem Statistics

This page shows various statistics and current usage information of the flash filesystem.

To view filesystem statistics:

1. Select Filesystem on the menu bar. The Filesystem page opens and shows the current filesystem statistics and usage.

To compact or format the filesystem:

1. Back up all files as necessary.
2. Select Filesystem on the menubar, if you are not already in the Filesystem page.
3. Click Compact in the Actions row.

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

4. Back up all files before you perform the next (Format) step, because all user files get erased in that step.
5. Click Format in the Actions row. The configuration gets retained.

---

**Figure 12-1 Filesystem Statistics**

<table>
<thead>
<tr>
<th>Statistics</th>
<th>Browse</th>
</tr>
</thead>
</table>

**Filesystem Statistics**

- **Filesystem Size:** 7,600,000 bytes (7,843,300 bytes)
- **Available Space:** 7,474,250 bytes (7,837,300 bytes) (99%)
- **Clean Space:** 7,335,300 bytes (7,692,072 bytes) (97%)
- **Dirty Space:** 140,064 bytes (144,328 bytes) (1%)
- **File & Dir Space Used:** 26,367 Kbytes (27,000 bytes) (0%)
- **Data Space Used:** 22,650 Kbytes (23,194 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 - 07, 9 erase cycles
- **Bank A Sectors:** 00 - 07, 0 erase cycles
- **Bank B Sectors:** 08 - 127, 2 erase cycles
- **Busy:** No

**Actions:** [Compact] [Format]
Filesystem Browser

To browse the filesystem:

1. Select **Filesystem** on the menu bar and then **Browse** at the top of the page. The Filesystem Browser page opens.

2. Select a filename to view the contents.
3. Click the X next to a filename to delete the file or directory. You can only delete a directory if it is empty.

4. Enter or modify the following settings:

   **Note:** Changes apply to the current directory view. To make changes within other folders, select the folder or directory and then enter the parameters in the settings listed below.

### Table 12-3 Filesystem Browser

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

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

TCP Settings

To configure the TCP network protocol:

1. Select Protocol Stack on the menu bar.
2. Select TCP.

3. Modify the following settings:

Table 12-5  TCP Protocol Settings

<table>
<thead>
<tr>
<th>Protocol Stack TCP Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Send RSTs</td>
<td>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. <strong>Note:</strong> Setting the RSTs may pose a security risk.</td>
</tr>
<tr>
<td>Ack Limit</td>
<td>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.</td>
</tr>
<tr>
<td>Send Data</td>
<td>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.</td>
</tr>
</tbody>
</table>
12: Maintenance and Diagnostics Settings

To configure the network protocol settings for IP:

1. Select Protocol Stack on the menu bar.
2. Select IP.

3. Modify the following settings:

<table>
<thead>
<tr>
<th>Protocol Stack TCP Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max Retrans</td>
<td>Enter the maximum number of retransmissions of a packet that will be attempted before failing.</td>
</tr>
<tr>
<td>Max Retrans Syn/Ack</td>
<td>Enter the maximum number of retransmissions of a SYN that will be attempted before failing. It is lower than “Max Retrans” to thwart denial-of-service attacks.</td>
</tr>
<tr>
<td>Max Timeout</td>
<td>Enter the maximum time between retransmissions.</td>
</tr>
</tbody>
</table>

4. Click Submit.

**IP Settings**

**To configure the network protocol settings for IP:**

1. Select Protocol Stack on the menu bar.
2. Select IP.

3. Modify the following settings:

<table>
<thead>
<tr>
<th>Protocol Stack TCP Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Time to Live</td>
<td>Enter the number of hops to be transmitted before the packet is discarded.</td>
</tr>
<tr>
<td>Multicast Time to Live</td>
<td>Enter the value to be greater than one to intentionally propagate multicast packets to additional routers.</td>
</tr>
</tbody>
</table>

4. Click Submit.
ICMP Settings

To configure the ICMP network protocol:

1. Select Protocol Stack on the menu bar.
2. Select ICMP.

3. Select the appropriate state.

Table 12-9  ICMP Settings

<table>
<thead>
<tr>
<th>Protocol Stack ICMP Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>The State selection is used to turn on/off processing of ICMP messages. This includes both incoming and outgoing messages. Choose Enabled or Disabled.</td>
</tr>
</tbody>
</table>

4. Click Submit.
ARP Settings

To configure the ARP network protocol:

1. Select **Protocol Stack** on the menu bar.
2. Select **ARP**.

3. Modify the following settings:

   **Table 12-11 ARP Settings**

<table>
<thead>
<tr>
<th>Protocol Stack ARP Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARP Timeout</td>
<td>This is the maximum duration an address remains in the cache. Enter the time, in <strong>hours</strong>, <strong>minutes</strong> and <strong>seconds</strong>.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Enter the IP address to add to the ARP cache.</td>
</tr>
</tbody>
</table>
Table 12-11 ARP Settings

<table>
<thead>
<tr>
<th>Protocol Stack ARP Settings (continued)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Address</td>
<td>Enter the MAC address to add to the ARP cache.</td>
</tr>
</tbody>
</table>

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

4. Click Submit for ARP or Add after supplying both address fields for ARP cache.

5. Remove entries from the ARP cache, as desired:
   - Click Remove All to remove all entries in the ARP cache.
   OR
   - Click Remove beside a specific entry to remove it from the ARP cache.

SMTP Settings

SMTP is configuration for a basic SMTP proxy. An SMTP proxy in this sense is a simple forwarding agent.

Note: Lantronix does not support SMTP AUTH or any other authentication or encryption schemes for email. Please see Email Settings for additional information.

To configure the SMTP network protocol:

1. Select Protocol Stack on the menu bar.
2. Select SMTP.

3. Modify the following settings:

Table 12-13 SMTP Settings

<table>
<thead>
<tr>
<th>Protocol Stack SMTP Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Relay Address</td>
<td>Address of all outbound email messages through a mail server. Can contain either a hostname or an IP address.</td>
</tr>
<tr>
<td>Remote Port</td>
<td>Port utilized for the delivery of outbound email messages.</td>
</tr>
</tbody>
</table>
4. Click **Submit**.

**IP Address Filter**

The IP address filter specifies the hosts and subnets permitted to communicate with the MatchPort AR embedded device server. When the filter list is empty, then all IP addresses are allowed.

*Note:* If using DHCP/BOOTP, ensure the DHCP/BOOTP server is in this list.

**To configure the IP address filter:**

1. Select **IP Address Filter** on the menu bar. The IP Address Filter page opens to display the current configuration.

2. Enter or modify the following settings:

   **Table 12-15 IP Address Filter Settings**

<table>
<thead>
<tr>
<th>IP Address Filter Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>Enter the IP address to add to the IP filter table.</td>
</tr>
<tr>
<td>Network Mask</td>
<td>Enter the IP address’ network mask in dotted notation.</td>
</tr>
</tbody>
</table>

3. Click **Add**.

*Note:* In the **Current State** table, click **Remove** to delete any existing settings, as necessary.
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 Using DeviceInstaller (on page 22).

To configure the query port server:

1. Select Query Port on the menu bar. The Query Port page opens to display the current configuration.

2. Select On to enable the query port server.

3. Click Submit.
Diagnostics

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

- Hardware
- MIB-II
- IP Sockets
- Ping
- Traceroute

*Note:* Lines 3 and 4 do not apply for MatchPort AR embedded device server.

- Log
- Memory
- Buffer Pools
- Processes

Hardware

This read-only page shows the current device’s hardware configuration.

To display hardware diagnostics:

1. Select Diagnostics on the menu bar. The Diagnostics: Hardware page opens and shows the current hardware configuration.
MIB-II Statistics

The MIB-II Network Statistics page shows the various SNMP-served Management Information Bases (MIBs) available on the MatchPort AR embedded device server.

To view MIB-II statistics:

1. Select Diagnostics on the menu bar and then MIB-II at the top of the page menu. The MIB-II Network Statistics page opens.

2. Click any of the available links to open the corresponding table and statistics. For more information, refer to the table below:

Requests for Comments (RFCs)

<table>
<thead>
<tr>
<th>RFC</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1213</td>
<td>Original MIB-II definitions.</td>
</tr>
<tr>
<td>2011</td>
<td>Updated definitions for IP and ICMP.</td>
</tr>
<tr>
<td>2012</td>
<td>Updated definitions for TCP.</td>
</tr>
<tr>
<td>2013</td>
<td>Updated definitions for UDP.</td>
</tr>
<tr>
<td>2096</td>
<td>Definitions for IP forwarding.</td>
</tr>
</tbody>
</table>
IP Sockets

To display open IP sockets:

1. Select Diagnostics on the menu bar and then IP Sockets at the top of the page. The IP Sockets page opens and shows all of the open IP sockets on the device.

![Figure 12-19 IP Sockets](image)

<table>
<thead>
<tr>
<th>Protocol</th>
<th>PkG</th>
<th>Tsk</th>
<th>LocalAddr:Port</th>
<th>RemoteAddr:Port</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>UDP</td>
<td>0</td>
<td>0</td>
<td>172.19.100.192:161</td>
<td>255.255.255.0</td>
<td>LISTEN</td>
</tr>
<tr>
<td>TCP</td>
<td>0</td>
<td>0</td>
<td>172.19.100.198:21</td>
<td>255.255.255.0</td>
<td>LISTEN</td>
</tr>
<tr>
<td>UDP</td>
<td>0</td>
<td>0</td>
<td>172.19.100.102:69</td>
<td>255.255.255.0</td>
<td>LISTEN</td>
</tr>
<tr>
<td>UDP</td>
<td>0</td>
<td>0</td>
<td>172.19.100.198:514</td>
<td>172.19.38.23:514</td>
<td>ESTABLISHED</td>
</tr>
<tr>
<td>TCP</td>
<td>0</td>
<td>0</td>
<td>172.19.100.198:80</td>
<td>255.255.255.0</td>
<td>LISTEN</td>
</tr>
<tr>
<td>UDP</td>
<td>0</td>
<td>0</td>
<td>172.19.100.198:30716</td>
<td>172.19.229.97:12770</td>
<td>ESTABLISHED</td>
</tr>
<tr>
<td>TCP</td>
<td>0</td>
<td>0</td>
<td>172.19.100.198:23</td>
<td>255.255.255.255.0</td>
<td>LISTEN</td>
</tr>
<tr>
<td>TCP</td>
<td>0</td>
<td>4</td>
<td>172.19.100.198:80</td>
<td>172.19.250.250:1844</td>
<td>ESTABLISHED</td>
</tr>
</tbody>
</table>

Ping

MatchPort AR embedded device server uses 56 bytes of data in a ping packet. Ping size is not configurable.

To ping a remote device or computer:

1. Select Diagnostics on the menu bar and then Ping at the top of the page. The Diagnostics: Ping page opens.
2. Enter or modify the following settings:

<table>
<thead>
<tr>
<th>Diagnostics: Ping Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>Enter the IP address or host name for the device to ping.</td>
</tr>
<tr>
<td>Count</td>
<td>Enter the number of ping packets the device should attempt to send to the Host. The default is 3.</td>
</tr>
<tr>
<td>Timeout</td>
<td>Enter the time, in seconds, for the device to wait for a response from the host before timing out. The default is 5 seconds.</td>
</tr>
</tbody>
</table>

3. Click **Submit**. The results of the ping display in the page.

**Traceroute**

Here you can trace a packet from the MatchPort AR unit 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:**

1. Select **Diagnostics** on the menu bar and then **Traceroute** at the top of the page. The Diagnostics: Traceroute page opens.
2. Enter or modify the following setting:

<table>
<thead>
<tr>
<th>Table 12-23 Diagnostics: Traceroute</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Diagnostics: Traceroute Settings</strong></td>
</tr>
<tr>
<td>Host</td>
</tr>
</tbody>
</table>

3. Click **Submit**. The results of the traceroute display in the page.

**Log**

Here you can enable a diagnostics log of configuration items:

**To use diagnostics logging:**

1. Select **Diagnostics** on the menu bar and then **Log** at the top of the page. The Diagnostics: Log page opens.
2. Select the **Output** type and select one of the following:
   - Disable (default)
   - Filesystem
   - Line1
   - Line 2

![Figure 12-25 Diagnostics: Log (Filesystem)](image1)

![Figure 12-26 Diagnostics: Log (Line 1)](image2)

**Memory**

This read-only web page shows the total memory and available memory (in bytes), along with the number of fragments, allocated blocks, and memory status.

**To display memory statistics:**

1. Select **Diagnostics** on the menu bar and then **Memory** at the top of the page. The Diagnostics: Memory page appears.
Diagnostics: Memory

<table>
<thead>
<tr>
<th></th>
<th>Main Heap</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Memory (bytes):</td>
<td>8313620</td>
</tr>
<tr>
<td>Available Memory (bytes):</td>
<td>3132304</td>
</tr>
<tr>
<td>Number Of Fragments:</td>
<td>9</td>
</tr>
<tr>
<td>Largest Fragment Avail:</td>
<td>3123656</td>
</tr>
<tr>
<td>Allocated Blocks:</td>
<td>1600</td>
</tr>
<tr>
<td>Number Of Alloc Fails:</td>
<td>0</td>
</tr>
<tr>
<td>Status:</td>
<td>OK</td>
</tr>
</tbody>
</table>

Buffer Pools

Several parts of the MatchPort AR system use private buffer pools to ensure deterministic memory management.

*To display the buffer pools:*

1. Select Diagnostics on the menu bar and then Buffer Pools at the top of the page. The Diagnostics: Buffer Pools page opens.

Diagnostics: Buffer pools

<table>
<thead>
<tr>
<th>Network Stack Buffer Pool</th>
<th>Total</th>
<th>Free</th>
<th>Used</th>
<th>MaxUsed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Buffer Headers</td>
<td>512</td>
<td>510</td>
<td>2</td>
<td>11</td>
</tr>
<tr>
<td>Cluster Pool Size: 2048</td>
<td>256</td>
<td>254</td>
<td>2</td>
<td>9</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Ethernet Driver Buffer Pool</th>
<th>Total</th>
<th>Free</th>
<th>Used</th>
<th>MaxUsed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Buffer Headers</td>
<td>2048</td>
<td>1984</td>
<td>64</td>
<td>70</td>
</tr>
<tr>
<td>Cluster Pool Size: 2048</td>
<td>1024</td>
<td>960</td>
<td>64</td>
<td>69</td>
</tr>
</tbody>
</table>
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 running and their associated statistics:

1. Select Diagnostics on the menu bar and then Processes at the top of the page.

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

The MatchPort AR System web page allows for rebooting the device, restoring factory defaults, uploading new firmware, configuring the short and long name, and viewing the current system configuration.

To configure system settings:

1. Select System on the menu bar. The System page opens.

2. Configure the following settings:

Table 12-31 System

<table>
<thead>
<tr>
<th>System Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reboot Device</td>
<td>Click Reboot to reboot the device. The system refreshes and redirects the browser to the device home page.</td>
</tr>
<tr>
<td>Restore Factory Defaults</td>
<td>Click Factory Defaults to restore the device to the original factory settings. All configurations will be lost. The device automatically reboots upon setting back to the defaults.</td>
</tr>
</tbody>
</table>
Upload New Firmware

Click **Browse** to locate the firmware file location. Click **Upload** to install the firmware on the device. The device automatically reboots upon the installation of new firmware.

*Note:* Close and reopen the web manager browser upon a firmware update.

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.

*Note:* Additional information about long and short name customization is available in *Short and Long Name Customization on page 139 of Chapter 15: Branding the MatchPort AR Unit*.

3. Click **Submit**.
13: Advanced Settings

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

- Email Settings
- Command Line Interface Settings
- XML Settings

Email Settings

The MatchPort AR allows you to view and configure email alerts relating to the events occurring within the system. Please see SMTP Settings on page 111 for additional information.

Note: The following section describes the steps to configure Email 1; these steps also apply to the other Email instances.

Email Statistics

This read-only page shows various 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.

1. Select Email on the menu bar. The Email web page appears.
2. Select an email number at the top of the page.
3. Select Statistics. The Email Statistics page for the selected email appears.
4. Repeat above steps as desired, according to additional email(s) available.

Figure 13-1 Email Statistics
Email Configuration

The MatchPort AR embedded device server allows you to view and configure email alerts relating to the events occurring within the system.

To configure email settings:

1. Select Email on the menu bar, if you are not already at the Email web page.
2. Select an email at the top of the page.
3. Select the Configuration submenu. The Email Configuration page opens to display the current email configuration.

4. Enter or modify the following settings:

Table 13-3 Email Configuration

<table>
<thead>
<tr>
<th>Email – Configuration Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>To</strong></td>
<td>Enter the email address to which the email alerts will be sent. Multiple addresses are separated by semicolon (;). Required field if an email is to be sent.</td>
</tr>
</tbody>
</table>
### Email – Configuration Settings (continued)

<table>
<thead>
<tr>
<th><strong>Description</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CC</strong></td>
<td>Enter the email address to which the email alerts will be copied. Multiple addresses are separated by semicolon (;).</td>
</tr>
<tr>
<td><strong>From</strong></td>
<td>Enter the email address to list in the From field of the email alert. Required field if an email is to be sent.</td>
</tr>
<tr>
<td><strong>Reply-To</strong></td>
<td>Enter the email address to list in the Reply-To field of the email alert.</td>
</tr>
<tr>
<td><strong>Subject</strong></td>
<td>Enter the subject for the email alert.</td>
</tr>
<tr>
<td><strong>Message File</strong></td>
<td>Enter the path of the file to send with the email alert. This file appears within the message body of the email.</td>
</tr>
<tr>
<td><strong>Overriding Domain</strong></td>
<td>Enter the domain name to override the current domain name in EHLO (Extended Hello).</td>
</tr>
<tr>
<td><strong>Server Port</strong></td>
<td>Enter the SMTP server port number. The default is port 25.</td>
</tr>
<tr>
<td><strong>Local Port</strong></td>
<td>Enter the local port to use for email alerts. The default is a random port number.</td>
</tr>
<tr>
<td><strong>Priority</strong></td>
<td>Select the priority level for the email alert.</td>
</tr>
<tr>
<td><strong>Trigger Email Send</strong></td>
<td>Configure these fields to send an email based on a CP Group trigger. The device sends an email when the specified Value matches the current Group’s value. The Value field appears once the CP Group is identified.</td>
</tr>
</tbody>
</table>

5. Click **Submit**.

   To test your configuration:
   
   a. Send an email immediately by clicking **Send Email** at the top of the page.
   b. Refer back to the Statistics page for a log of the transaction.

6. Repeat above steps as desired, according to additional email(s) available.
Command Line Interface Settings

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.

CLI Statistics

This read-only page shows the current connection status of the CLI servers listening on the Telnet and SSH ports. When a connection is active, the following display:

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

To view the CLI Statistics:


CLI Configuration

On this page you can change CLI settings.

To configure the CLI:

1. Select CLI on the menu and then Configuration at the top of the page. The Command Line Interface Configuration page appears.
2. Enter or modify the following settings:

<table>
<thead>
<tr>
<th>Command Line Interface Configuration Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login Password</td>
<td>Enter the password for Telnet access.</td>
</tr>
<tr>
<td>Enable Level Password</td>
<td>Enter the password for access to the Command Mode Enable level. There is no password by default.</td>
</tr>
</tbody>
</table>
| Quit Connect Line                             | Enter a string to terminate a connect line session and resume the CLI. Type `<control>l` 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. |
| Telnet Max Sessions                           | Maximum number of simultaneous Telnet sessions. The default is 3 and the maximum is 10. |
| 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. The default is 3 and the maximum is 10. |

3. Click Submit.
XML Settings

MatchPort AR embedded device server allows for the configuration of devices by using XML configuration records (XCRs). You can export an existing configuration for use on other devices 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. 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:

\(<g>:\langle i\rangle;\langle g\>:\langle i\rangle;\ldots\)

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 \(<g>:\langle i\rangle\) value is separated with a semicolon. If a group has no instance, specify the group name \(<g>\) only.

The number of lines available for importing and exporting differ between Lantronix products. The screenshots in this chapter represent one line, as available, for example, on an XPort Pro embedded networking module and EDS1100. However, other device networking products (such as EDS2100, EDS4100, XPort AR, MatchPort AR embedded networking modules, EDS8/16PS and EDS8/16/32PR) support additional lines.
XML: Export Configuration

On this web page you can export the current system configuration in XML format.

To export the system configuration:


   The number of Lines to Export and the specific Groups to Export displayed on your screen may vary according to your particular product.

2. Enter or modify the following settings:

   Note: Number of lines and groups available for export configuration vary between Lantronix products.

3. Click Export. The groups display if exporting the data to the browser. If exporting the data to a local file, the file is stored on the file system.

<table>
<thead>
<tr>
<th>XML Export Configuration Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Export to browser</td>
<td>Select this option to export the XCR data in the selected fields to a web browser.</td>
</tr>
<tr>
<td>Export to local file</td>
<td>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.</td>
</tr>
<tr>
<td>Export secrets</td>
<td>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.</td>
</tr>
<tr>
<td>Lines to Export</td>
<td>Select the instances you want to export in the line, tunnel, and terminal groups.</td>
</tr>
<tr>
<td>Groups to Export</td>
<td>Check the configuration groups that are to be exported to the XML configuration record.</td>
</tr>
</tbody>
</table>

Table 13-8  XML Export Configuration
**XML: Export Status**

On this page you can export the current system status in XML format. The XML data can be exported to the browser page or to a file on the file system.

**To export the system status:**

1. Select XML on menu bar and then Export Status at the top of the page. The XML: Export Status page appears.

   The number of Lines to Export and the specific Groups to Export displayed on your screen may vary according to your particular product.

2. Enter or modify the following settings:

   **Note:** Number of lines and groups available for export vary between Lantronix products.

3. Click Export. The groups display if exporting the data to the browser. If exporting the data to a local file system, the file is stored on the file system.

   **Note:** Most browsers will interpret and display the XML data without the XML tags. To view the raw XML, choose the view file source feature of your browser.

---

### Table 13-10 XML Export Status

<table>
<thead>
<tr>
<th>XML: Export System Status Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Export to browser</td>
<td>Select this option to export the XML status record to a web browser.</td>
</tr>
<tr>
<td>Export to local file</td>
<td>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.</td>
</tr>
<tr>
<td>Lines to Export</td>
<td>Select the instances you want to export in the line, tunnel, and terminal groups.</td>
</tr>
<tr>
<td>Groups to Export</td>
<td>Check the configuration groups that are to be exported into the XML status record.</td>
</tr>
</tbody>
</table>

**Note:** Most browsers will interpret and display the XML data without the XML tags. To view the raw XML, choose the view file source feature of your browser.
XML: Import Configuration

Here 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>;` Each `<g>:<i>` value is separated with a semicolon. If a group has no instance, specify the group name `<g>` only.

To import a system configuration:

1. Select XML on the menu bar and then Import Configuration at the top of the page. The XML: Import Configuration web page appears.

2. Click one of the following radio buttons:
   - Configuration from External file. See Import Configuration from External File on page 132.
   - Configuration from Filesystem. See Import Configuration from the Filesystem on page 133.
   - Line(s) from single line Settings on the Filesystem. See Import Line(s) from Single Line Settings on the Filesystem on page 135.

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.
Import Configuration from the Filesystem

This selection shows a page for entering the filesystem and your import requirements – groups, lines, and instances. The number of Lines to Import and the specific Whole Groups to Import displayed on your screen may vary according to your particular product.

**Figure 13-13 XML: Import from Filesystem**

**XML: Import Configuration**

Import configuration from the filesystem:

- **Filename**: [Enter Filename]

- **Lines to Import**: [Clear All] [Select All]

- **Whole Groups to Import**: [Clear All] [Select All but Networking]

- **XML Elements**:
  - tftp
  - device
  - ethernet
  - http server
  - ip
  - ipd
  - ppp
  - serial command mode
  - ssh
  - ssh client
  - sftp
  - telnet
  - tunnel accept
  - tunnel mode
  - wp
  - cli
  - diagnostics
  - execute
  - icmp
  - igi
  - ifilter
  - ManageLinux
  - query port
  - smtp
  - ssh client
  - syslog
  - terminal
  - tunnel connect
  - tunnel disconnect
  - tunnel packing
  - tunnel serial
  - tcp
  - telnet
  - http authentication
  - interface
  - line
  - modbus
  - rss
  - snmp
  - cp group
  - email
  - exit cli
  - http authentication url
  - import

- **Text List**: [Enter Text]

- **Import**: [Import Button]
1. Enter or modify the following settings.

Figure 13-14 XML: Import Configuration from Filesystem

<table>
<thead>
<tr>
<th>Import Configuration from Filesystem Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filename</td>
<td>Enter the name of the file on the device (local to its filesystem) that contains XCR data.</td>
</tr>
<tr>
<td>Lines to Import</td>
<td>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, tunnel, and terminal groups.</td>
</tr>
<tr>
<td>Whole Groups to Import</td>
<td>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.</td>
</tr>
</tbody>
</table>
| 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. |

2. 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. The number of **Lines to Import** and the specific **Whole Groups to Import** displayed on your screen may vary according to your particular product.

**To modify Single Line Settings on the Filesystem:**

Figure 13-15 XML: Import Line(s) from Single Line Settings on the Filesystem

<table>
<thead>
<tr>
<th>Export Configuration</th>
<th>Export Status</th>
<th>Import Configuration</th>
</tr>
</thead>
</table>

**XML: Import Configuration**

- **Filename**

- **Lines to Import:** [Clear All] [Select All]
  - 1
  - network

- **Whole Groups to Import:** [Clear All] [Select All but Networking]
  - arp
  - device
  - athwlan
  - ftp server
  - http server
  - ip
  - ip6
  - ipv6
  - serial command mode
  - ssh
  - ssl
  - telnet
  - tunnel accept
  - tunnel modem
  - vip
  - cli
  - diagnostics
  - execute
  - host
  - icmp
  - ip filter
  - ManageLinux
  - query port
  - smtp
  - ssh client
  - syslog
  - terminal
  - tunnel connect
  - tunnel packing
  - xml import control
  - cp group
  - email
  - exit cli
  - http authentication uri
  - interface
  - line
  - modbus
  - ros
  - snmp
  - ssh server
  - tcp
  - http server
  - tunnel disconnect
  - tunnel serial

- **Import**
1. Enter or modify the following settings:

<table>
<thead>
<tr>
<th>Table 13-16 XML: Import Line(s) from Single Line Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Import Line(s) Settings</strong></td>
</tr>
<tr>
<td>Filename</td>
</tr>
<tr>
<td>Lines to Import</td>
</tr>
</tbody>
</table>
| 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. |

2. Click Import.
14: Security in Detail

Public Key Infrastructure

Public key infrastructure (PKI) is based on an encryption technique that uses two keys: a public key and private key. Public keys can be used to encrypt messages which can only be decrypted using the private key. This technique is referred to as asymmetric encryption, as opposed to symmetric encryption, in which a single secret key is used by both parties.

TLS (SSL)

Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), use asymmetric encryption for authentication. In some scenarios, only a server needs to be authenticated, in others both client and server authenticate each other. Once authentication is established, clients and servers use asymmetric encryption to exchange a secret key. Communication then proceeds with symmetric encryption, using this key.

SSH and some wireless authentication methods on the MatchPort AR embedded device server make use of SSL. The MatchPort AR unit supports SSLv2, SSLv3, and TLS1.0.

TLS/SSL application hosts use separate digital certificates as a basis for authentication in both directions: to prove their own identity to the other party, and to verify the identity of the other party. In proving its own authenticity, the MatchPort AR embedded device server will use its own "personal" certificate. In verifying the authenticity of the other party, the MatchPort AR unit will use a "trusted authority" certificate.

Digital 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. With digital certificates, a cryptographic key is used to create a unique digital signature.

Trusted Authorities

A private key is used by a trusted certificate authority (CA) to create a unique digital signature. Along with this private key is a certificate of authority, containing a matching public key that can be used to verify the authority's signature but not re-create it.

A chain of signed certificates, anchored by a root CA, can be used to establish a sender's authenticity. Each link in the chain is certified by a signed certificate from the previous link, with the exception of the root CA. This way, trust is transferred along the chain, from the root CA through any number of intermediate authorities, ultimately to the agent that needs to prove its authenticity.
Obtaining Certificates

Signed certificates are typically obtained from well-known CAs, such as VeriSign. This is done by submitting a certificate request for a CA, typically for a fee. The CA will sign the certificate request, producing a certificate/key combo: the certificate contains the identity of the owner and the public key, and the private key is available separately for use by the owner.

As an alternative to acquiring a signed certificate from a CA, you can act as your own CA and create self-signed certificates. This is often done for testing scenarios, and sometimes for closed environments where the expense of a CA-signed root certificate is not necessary.

Self-Signed Certificates

A few utilities exist to generate self-signed certificates or sign certificate requests. The MatchPort AR embedded device server 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 unit.

Certificate Formats

Certificates and private keys can be stored in several file formats. The best known formats are PKCS12, DER and PEM. Certificate and key can be in the same file or in separate files. Additionally, the key can either be encrypted with a password or left in the clear. However, the MatchPort AR embedded device server currently only accepts separate PEM files, with the key unencrypted.

Several utilities exist to convert between the formats.

OpenSSL

OpenSSL is a widely used open source set of SSL related command line utilities. It can act as server or client. It can also generate or sign certificate requests, and can convert from and to several different of formats.

OpenSSL is available in binary form for Linux and Windows.

To generate a self-signed RSA certificate/key combo:

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

See www.openssl.org or www.madboa.com/geek/openssl for more information.

**Note:** Signing other certificate requests is also possible with OpenSSL but the details of this process are outside the scope of this document.
15: Branding the MatchPort AR Unit

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

- Web Manager Customization
- Short and Long Name Customization

Web Manager Customization

Customize the Web Manager's appearance by modifying index.html and style.css. The style (fonts, colors, and spacing) of the Web Manager is 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 AR embedded device server file system.

Web Manager files can be retrieved and overridden with the following procedure:

1. FTP to the MatchPort AR device.
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 appear in the file system's http/config directory.
8. Restart any open browser to view the changes.
9. If you wish to go back to the default files in the firmware image, simply delete the overriding files from the file system.

Short and Long Name Customization

Short and long names may be customized in Web Manager according to the directions in System Settings. 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
```

The long and short names appear in the Product Type field in the following format:

```
Product Type: <long name> (<short name>)
```

For example:

```
(enable)# show
Product Information:
Product Type: Lantronix MatchPort AR (MatchPort AR)
```
16: Updating Firmware

Obtaining Firmware

Obtain up-to-date firmware and release notes for the unit from the Lantronix web site (http://www.lantronix.com/support/downloads) or by using anonymous FTP (ftp://ftp.lantronix.com/).

Loading New Firmware

Reload the firmware using the device web manager Filesystem page.

To upload new firmware:


   ![Figure 16-1 Update Firmware]

2. Click Browse to browse to the firmware file.
3. Highlight the file and click Open.
4. Click Upload to install the firmware on the MatchPort AR embedded device server. The device automatically reboots on the installation of new firmware.
5. Close and reopen the web manager internet browser to view the device's updated web pages.

   Note: Alternatively, firmware may be updated by sending the file to the MatchPort AR embedded device server over a FTP or TFTP connection.
Appendix A: Technical Support

If you are unable to resolve an issue using the information in this documentation, please contact Technical Support.

North America

Hours: 6:00am - 5:00pm Pacific Time
Mon. - Fri. (excluding holidays)

www.lantronix.com/support/
FTP: ftp.lantronix.com
Tel: (800) 422-7044 (US Only)
Tel: (949) 453-7198
Fax: (949) 450-7226

Europe, Middle East, Africa (EMEA)

www.lantronix.com/support/
Tel: +31 (0)76 52 36 740

Japan

japan_sales@lantronix.com
Tel: +81-3-6277-8802

Asia / Pacific (APAC)

asiapacific_sales@lantronix.com
Tel: + 852 3428-2338

Latin America & Caribbean

la_sales@lantronix.com
Tel: +1 949 453 3990
Online

Support options listed below are available 24 hours a day, 7 days a week at the Lantronix support page at http://www.lantronix.com/support

- Download firmware
- Search and review Frequently asked Questions (FAQs)
- Send a question to technical 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/MAC address
- 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 exported XML Configuration file.
Appendix B: Compliance

(According to ISO/IEC Guide

Manufacturer’s Name & Address:
Lantronix, Inc. 167 Technology Drive, Irvine, CA 92618 USA

Product Name Model:
MatchPort® AR Embedded Device Server

Conform 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
EN61000-3-2: 2000 + A2: 2005

Immunity

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
**Manufacturer’s Contact:**

Lantronix, Inc.
167 Technology Drive, Irvine, CA 92618 USA
Tel: 949-453-3990
Fax: 949-453-3995

---

**RoHS Notice**

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

<table>
<thead>
<tr>
<th>Product Family Name</th>
<th>Toxic or hazardous Substances and Elements</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Lead (Pb)</td>
</tr>
<tr>
<td>UDS1100 and 2100</td>
<td>0</td>
</tr>
<tr>
<td>EDS</td>
<td>0</td>
</tr>
<tr>
<td>MSS100</td>
<td>0</td>
</tr>
<tr>
<td>IntelliiBox</td>
<td>0</td>
</tr>
<tr>
<td>XPress DR &amp; XPress-DR+</td>
<td>0</td>
</tr>
<tr>
<td>SecureBox 1101 &amp; 2101</td>
<td>0</td>
</tr>
<tr>
<td>WiBox</td>
<td>0</td>
</tr>
<tr>
<td>UBox</td>
<td>0</td>
</tr>
<tr>
<td>MatchPort</td>
<td>0</td>
</tr>
<tr>
<td>SLC</td>
<td>0</td>
</tr>
<tr>
<td>XPort</td>
<td>0</td>
</tr>
<tr>
<td>WiPort</td>
<td>0</td>
</tr>
<tr>
<td>SLB</td>
<td>0</td>
</tr>
<tr>
<td>SLP</td>
<td>0</td>
</tr>
<tr>
<td>SCS</td>
<td>0</td>
</tr>
<tr>
<td>SLS</td>
<td>0</td>
</tr>
<tr>
<td>DSC</td>
<td>0</td>
</tr>
<tr>
<td>PremierWave</td>
<td>0</td>
</tr>
<tr>
<td>Micro125</td>
<td>0</td>
</tr>
</tbody>
</table>

O: 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.
Appendix C: Binary to Hexadecimal Conversions

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

Use this chapter to learn to convert binary values to hexadecimals 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

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>
<thead>
<tr>
<th>Decimal</th>
<th>Binary</th>
<th>Hex</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0000</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0001</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>0010</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>0011</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>0100</td>
<td>4</td>
</tr>
<tr>
<td>5</td>
<td>0101</td>
<td>5</td>
</tr>
<tr>
<td>6</td>
<td>0110</td>
<td>6</td>
</tr>
<tr>
<td>7</td>
<td>0111</td>
<td>7</td>
</tr>
<tr>
<td>8</td>
<td>1000</td>
<td>8</td>
</tr>
<tr>
<td>9</td>
<td>1001</td>
<td>9</td>
</tr>
<tr>
<td>10</td>
<td>1010</td>
<td>A</td>
</tr>
<tr>
<td>11</td>
<td>1011</td>
<td>B</td>
</tr>
<tr>
<td>12</td>
<td>1100</td>
<td>C</td>
</tr>
<tr>
<td>13</td>
<td>1101</td>
<td>D</td>
</tr>
<tr>
<td>14</td>
<td>1110</td>
<td>E</td>
</tr>
<tr>
<td>15</td>
<td>1111</td>
<td>F</td>
</tr>
</tbody>
</table>
**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.

![Scientific Calculator](image1)

4. Click Hex. The hexadecimal value appears.

![Scientific Calculator](image2)
Appendix D: Warranty

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

A
Accept Mode 37
Accept Mode 43
Additional Documentation 15
Additional TCP Server Port 103
Address
  Ethernet 20
  Hardware 20, 21
  IP 20
  MAC 20, 21
Advanced Settings
  Email Configuration 125
  XML Configuration 129
Advanced Settings 124
AES 17
Allow Firmware Update 72
Allow TFTP File Creation 72
Allow XCR Import 72
ARP 17
ARP Settings 110, 111
ASCII 99
Auth Type 78
Authentication Mode 69
Authentication Type 78
Authority 97
AutoIP 17

B
Banner 81
Bar Code 21
Bin 146
Binary 61, 81, 145
Binary to Hexadecimal Conversions 145
Bit 61, 64
Block Network 44, 49
Block Serial 49
Block Serial Data 44
BOOTP 17, 30
Branding 139
  Web Manager Customization 139
Break Duration 57

C
Challenge Handshake Authentication Protocol 67
CHAP 67
CLI 18
CLI Configuration 127
CLI Statistics 127
Command Line Interface Settings 127
Command Mode 20
Command-Line Interface 18
Common Name 98
Compliance 143
Configurable Pin Manager 59
Configuration Methods 20
Configuration Settings 66
Configured As 61
Connect Mode 37
Connect Mode 46
Connection Value 45
Convert Newlines 82
Count 117
CP 61
CP Output 45, 49
CPM 59
Create New Keys 92
Create New Self-Signed Certificate 97
Custom Groups 59

D
Default Gateway 31
Default Groups 59
Default Server Port Numbers 20
Device Control 18
Device Details 22
Device Details Summary 22
Device Management 19
Device Status 25
DeviceInstaller 22
DeviceInstaller 22
DHCP 17, 31
Diagnostic Toolset 19
Diagnostics 114
  Buffer Pools 120
  Hardware 114
  IP Sockets 116
  Memory 119
  MIB-II Statistics 115
  Ping 116
  Processes 121
Diagnostics Log 118
Diagnostics Settings 104
Disconnect Mode 37
Disconnect Mode 50
Disconnection Value 45
DNS 17, 31
DNS Settings 66
E
Echo 56, 57
Email on Connect 45, 49
Email on Disconnect 45, 49
Enable Level Password 128
Encryption 19
End of Job 81
Enterprise-Grade Security 18
EOJ String 82
Ethernet address 20
Evolution OS 17
Evolution OS™ 17
Exit Connect Menu 56, 57
Expires 98
Export Secrets 130
Export to Browser 130, 131
Export to Local File 130, 131

F
File System
  Browser 105
  Statistics 104
Filename 134, 136
Filesystem 27, 140
Firmware 140
Flush Serial Data 44, 49
Formfeed 82
FTP 17, 140
FTP Configuration 71

G
Groups to Export 130, 131

H
Hardware Address 20, 21
Help Area 26
Hex 146
Hexadecimal 145
Host 48, 106, 117, 118
Host Configuration 57
Host Configuration 57
Host IP Promotion 50
Hostname 31
HTTP 17
  Authentication 77
  Change Configuration 75
  Configuration 74
  Statistics 74

I
I/O 61
ICMP 17
ICMP Settings 109
Import Configuration from External File 132
Import Configuration from the Filesystem 133
Import Line(s) from Single Line Settings on the Filesystem 135
Inactivity Timeout 128
IP 17
  Address 20
  Address Filter 112
  Settings 108
ISO/IEC Guide 143

K
Key Features 16
Key Length 98
Key Type 85, 86, 92

L
Label 21
Lantronix Discovery Protocol 21
Level 61
Line 1
  Configuration 34
  Statistics 33
Line Settings 33
Lines to Export 130, 131
Lines to Import 134, 136
Loading New Firmware 140
Local IP Address 68
Local Port 44, 48
Logic 61
Login Connect Menu 56, 57
Login Password 128
Logout 26
LPD
  Configuration Page 81
  Settings 80
LPD Statistics 80
M
MAC Address 20, 21
Maintenance and Diagnostics Settings
  Protocol Stack 107
Maintenance Settings 104
Manufacturer’s Name & Address 143
Max Entries 79
Modbus Configuration 103
Modbus Statistics 102
Modbus 99
Modbus_Ctl_In 99
Modbus_Ctl_Out 99
Mode 48
Modem Emulation 18
Modem Emulation 52
MTU 31
Multiple Hosts 50

N
Name 123
NAT 67
Network 1 (eth0) Interface Configuration 30
Network 1 Ethernet Link 32
Network Address Translation 67
Network Settings
  Network 1 Interface Configuration 30
  Network 1 Interface Status 29
Network Settings 29
New Certificate 97
New Private Key 97

O
Obtaining Firmware 140
Organization Unit 97

P
Packing Mode 41
PAP 67
Password 45, 69, 92
Password Authentication Protocol 67
PBX 19
Peer IP Address 68
Persistent 79
Point-to-Point Protocol 67
Port 106
Port Numbers 20
Pports
  Serial and Telnet 20
PPP Peer Device 67
PPP Settings 67
Private Branch Exchange 19
Private Key 85, 86, 92
Product Information Label 21
Product Name Model 143
Product Revision 21
Protocol 44, 58
Protocol Support 17
Public Key 85, 86, 92

Q
Query Port 113
Queue Name 82
Quit Connect Line 128

R
Radiated and Conducted Emissions 143
Read Community 70
Really Simple Syndication 18
Reboot Device 122
Reconnect Timer 49
Ref 61
Remote Address 58
Remote Command 92
Remote Port 58
Response Timeout 103
Restore Factory Defaults 122
RFC1334 67
RoHS Notice 144
RSS 17, 18
RSS Feed 79
RSS Settings 79
RSS Trace Input 103
RTU 99

S
Scientific 146
Scientific Calculator 146
SCPR 19
Secure Com Port Redirector 19
Secure Shell 83
Secure Sockets Layer 83, 93
Security
  Enterprise-Grade 18
  Settings 83
Security Settings 83
SSL Certificates and Private Keys 94
SSL Cipher Suites 93
SSL RSAor DSA 94
SSL Utilities 95
Send Break 57
Settings
   Network 1 Ethernet Link 32
Write Community 70

X
XML 20
   Export Configuration 130
   Export Status 131
   Import System Configuration 132
XML-Based Architecture 18