

LANTRONIX®



**MatchPort® b/g Pro
Embedded Device Server
User Guide**

Part Number 900-531
Revision E June 2013

Copyright & Trademark

© 2013 Lantronix, Inc. All rights reserved. No part of the contents of this book may be transmitted or reproduced in any form or by any means without the written permission of Lantronix.

Lantronix®, XPort®, XPort AR®, and MatchPort® are registered trademarks of Lantronix, Inc. in the United States and other countries. Evolution OS® is a registered trademark of Lantronix, Inc. in the United States. DeviceInstaller™ is a trademark of Lantronix, Inc.

Windows® and Internet Explorer® are registered trademarks of Microsoft Corporation. Mozilla® and Firefox® are registered trademarks of the Mozilla Foundation. Chrome™ is a trademark of Google, Inc. Opera® is a registered trademark of Opera Software ASA Corporation Norway. All other trademarks and trade names are the property of their respective holders.

Contacts

Lantronix, Inc. Corporate Headquarters

167 Technology Drive
Irvine, CA 92618, USA
Phone: 949-453-3990
Fax: 949-453-3995

Technical Support

Online: www.lantronix.com/support

Sales Offices

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

Disclaimer

Note: This product has been designed to comply with the limits for a Class Rules when properly enclosed and grounded. These limits are designed to provide reasonable protection against such interference. This equipment generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with this guide, may cause interference to radio communications. See the appendix, [Compliance on page 161](#)

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

Revision History

Date	Rev.	Comments
April 2008	A	Initial Document
September 2008	B	Technical updates throughout, corresponding to release 1.1.0.R6.
March 2009	C	Updated to firmware version 1.3.0.0R9, includes bridging and roaming.
October 2011	D	Updated memory information.
June 2013	E	Updated to firmware version 5.2.0.3R2.

Table of Contents

Copyright & Trademark	2
Contacts	2
Disclaimer	2
Revision History	2
List of Tables	8
List of Figures	10
1: About This Guide	13
Chapter and Appendix Summaries	13
Additional Documentation	14
2: Introduction	15
Key Features	15
Applications	16
Protocol Support	16
Evolution OS	16
Additional Features	17
Modem Emulation	17
Web-Based Configuration and Troubleshooting	17
Command-Line Interface (CLI)	17
SNMP Management	17
XML-Based Architecture and Device Control	17
Really Simple Syndication (RSS)	17
Enterprise-Grade Security	17
Terminal Server/Device Management	18
Troubleshooting Capabilities	18
Configuration Methods	18
Addresses and Port Numbers	19
Hardware Address	19
IP Address	19
Port Numbers	19
Product Information Label	20
3: Using DeviceInstaller	21
Accessing MatchPort b/g Pro Using DeviceInstaller	21
Device Details Summary	21

4: Configuration Using Web Manager	23
Accessing Web Manager	23
Device Status Page	24
Web Manager Page Components	25
Navigating the Web Manager	26
5: Network Settings	28
Network 1 (eth0) Interface Status	28
Network 1 (eth0) Interface Configuration	29
Network 1 Ethernet Link	31
Network 2 (wlan0) Interface Status	32
Network 2 (wlan0) Interface Configuration	32
Network 2 (wlan0) WLAN Link Status	34
Network 2 (wlan0) WLAN Link Configuration	35
Network 2 (wlan0) WLAN Link Scan	36
WLAN Profiles	38
WEP Settings	40
WPA and WPA2/IEEE802.11i Settings	41
6: Line and Tunnel Settings	45
Line Settings	45
Line Statistics	45
Line Configuration	46
Line Command Mode	48
Tunnel Settings	49
Tunnel – Statistics	50
Tunnel – Serial Settings	52
Tunnel – Packing Mode	53
Tunnel – Accept Mode	55
Tunnel – Connect Mode	58
Tunnel – Disconnect Mode	62
Tunnel – Modem Emulation	64
7: Terminal and Host Settings	67
Terminal Settings	67
Line Terminal Configuration	67
Network Terminal Configuration	68
Host Configuration	69

8: Configurable Pin Manager	71
Overview	71
Default Groups	71
Custom Groups	71
CPM: CP (Configurable Pins)	71
View CPs	72
CPM: Groups	74
View Groups	74
9: Service Settings	78
DNS Settings	78
Point-to-Point (PPP) Settings	79
SNMP Settings	81
FTP Settings	82
TFTP Settings	83
Syslog Settings	84
HTTP Settings	86
HTTP Statistics	86
HTTP Configuration	87
HTTP Authentication	89
RSS Settings	91
LPD Settings	92
LPD Statistics	92
LPD Configuration	93
10: Security Settings	95
SSH Settings	95
SSH Server Host Keys	96
SSH Server Authorized Users	100
SSH Client Known Hosts	102
SSH Client Users	103
SSL Settings	105
SSL Cipher Suites	105
SSL Certificates	106
SSL RSA or DSA	106
SSL Certificates and Private Keys	106
SSL Utilities	107
SSL Configuration	108

11: Modbus	111
CP Control via Modbus	111
Serial Transmission Mode	113
Modbus Statistics	114
Modbus Configuration	115
12: Maintenance and Diagnostics Settings	116
Filesystem Settings	116
Filesystem Statistics	116
Filesystem Browser	117
Protocol Stack Settings	119
TCP Settings	119
IP Settings	120
ICMP Settings	121
ARP Settings	122
SMTP Settings	123
IP Address Filter	124
Query Port	125
Diagnostics	126
Hardware	126
MIB-II Statistics	127
IP Sockets	128
Ping	128
Traceroute	129
Log	130
Verbosity	132
Memory	132
Buffer Pools	133
Processes	134
System Settings	135
13: Advanced Settings	137
Email Settings	137
Email Statistics	137
Email Configuration	138
Command Line Interface Settings	140
CLI Statistics	140
CLI Configuration	140
XML Settings	142
XML: Export Configuration	143
XML: Export Status	144
XML: Import Configuration	145

CPU Power Management	149
14: Bridging	150
Bridging Configuration	150
Bridging Operation	151
Bridge Settings	151
Bridge 1 (bridge0) Status	151
Bridge 1 (bridge0) Configuration	154
15: Security in Detail	155
Public Key Infrastructure	155
TLS (SSL)	155
Digital Certificates	155
Trusted Authorities	155
Obtaining Certificates	156
Self-Signed Certificates	156
Certificate Formats	156
OpenSSL	156
Steel Belted RADIUS	157
Free RADIUS	157
16: Branding the MatchPort b/g Pro	158
Web Manager Customization	158
Short and Long Name Customization	158
17: Updating Firmware	159
Obtaining Firmware	159
Loading New Firmware	159
Appendix A: Technical Support	160
Appendix B: Compliance	161
Appendix C: Binary to Hexadecimal Conversions	163
Converting Binary to Hexadecimal	163
Conversion Table	163
Scientific Calculator	164
Appendix D: Warranty	165
Index	166

List of Tables

Table 3-1 Device Details Summary	21
Table 4-4 Summary of Web Manager Pages	26
Table 5-3 Network 1 (eth0) Interface Configuration	29
Table 5-5 Network 1 Ethernet Link	31
Table 5-8 Network 2 (wlan0) Interface Configuration	33
Table 5-11 Network 2 (wlan0) Interface Configuration	36
Table 5-13 Network 2 (wlan0) WLAN Link Scan	37
Table 5-14 Device Information within Range	37
Table 5-17 WLAN Profile Page Settings	39
Table 5-19 WLAN Profile Security - WEP Settings	41
Table 5-24 WPA and WPA2/IEEE802.11i Settings	43
Table 6-3 Line Configuration	47
Table 6-5 Line Command Mode	48
Table 6-8 Tunnel - Serial Settings	52
Table 6-12 Tunnel Packing Mode	55
Table 6-14 Tunnel Accept Mode	57
Table 6-16 Tunnel Connect Mode	60
Table 6-19 Tunnel Disconnect Mode	63
Table 6-20 Modem Emulation Commands and Descriptions	64
Table 6-22 Tunnel Modem Emulation	66
Table 7-2 Terminal on Line 1 Configuration	68
Table 7-4 Terminal on Network Configuration	69
Table 7-6 Host Configuration	70
Table 8-2 CPM CPs Current Configuration	73
Table 8-3 CPM CPs Status	73
Table 8-5 CPM Groups Current Configuration	75
Table 8-7 Group Status	76
Table 9-3 PPP Configuration	80
Table 9-5 SNMP	81
Table 9-7 FTP Settings	83
Table 9-9 TFTP Server	84
Table 9-11 Syslog	85
Table 9-14 HTTP Configuration	87
Table 9-16 HTTP Authentication	89
Table 9-18 RSS	91
Table 9-21 LPD Configuration	93

Table 10-2 SSH Server Host Keys Settings - Upload Keys Method	97
Table 10-4 SSH Server Host Keys Settings - Upload Keys Method	98
Table 10-6 SSH Server Host Keys Settings - Create New Keys Method	99
Table 10-8 SSH Server Authorized User Settings	101
Table 10-10 SSH Client Known Hosts	102
Table 10-12 SSH Client Users	104
Table 10-13 Supported Cipher Suites	105
Table 10-15 SSL	109
Table 11-1 6 Byte Header of Modbus Application Protocol	111
Table 11-2 Modbus Local Slave Functions - Query	111
Table 11-3 Modbus Local Slave Functions - Response	112
Table 11-4 Modbus Transmission Modes	113
Table 11-7 Modbus Configuration	115
Table 12-3 Filesystem Browser	118
Table 12-5 TCP Protocol Settings	119
Table 12-7 IP Protocol Settings	120
Table 12-9 ICMP Settings	121
Table 12-11 ARP Settings	122
Table 12-13 SMTP Settings	123
Table 12-15 IP Address Filter Settings	124
Table 12-19 Requests for Comments (RFCs)	127
Table 12-22 Diagnostics: Ping	129
Table 12-24 Diagnostics: Traceroute	130
Table 12-29 IP Address Filter Settings	132
Table 12-34 System	135
Table 13-3 Email Configuration	138
Table 13-6 CLI Configuration	141
Table 13-8 XML Export Configuration	143
Table 13-10 XML Export Status	144
Table 13-16 XML: Import Line(s) from Single Line Settings	149
Table 13-18 Modbus Configuration	149
Table 14-2 Status Page Items:	152
Table C-1 Binary to Hexadecimal Conversion Table	163

List of Figures

Figure 2-1 Sample Hardware Address	19
Figure 2-2 Product Label	20
Figure 4-1 Prompt for User Name and Password	23
Figure 4-2 Web Manager Home Page	24
Figure 4-3 Components of the Web Manager Page	25
Figure 5-1 Network 1 (eth0) Interface Status	28
Figure 5-2 Network 1 (eth0) Interface Configuration	29
Figure 5-4 Network 1 Ethernet Link	31
Figure 5-6 Network 2 (wlan0) Interface Status	32
Figure 5-7 Network 2 (wlan0) Interface Configuration	33
Figure 5-9 Network 2 (wlan0) WLAN Link Status	35
Figure 5-10 Network 2 (wlan0) WLAN Link Configuration	35
Figure 5-12 Network 2 (wlan0) WLAN Link Scan	37
Figure 5-15 WLAN Profiles	38
Figure 5-16 WLAN Profile Page	39
Figure 5-18 WLAN Profile Security -- WEP Settings	40
Figure 5-20 WLAN Profile Security – WPA with PSK Authentication	41
Figure 5-21 WLAN Profile Security – WPA2/IEEE 802.11i with PSK Authentication	42
Figure 5-22 WLAN Profile Security – WPA with IEEE 802.1X Authentication	42
Figure 5-23 WLAN Profile Security – WPA2/IEEE 802.11i with IEEE 802.1X Authentication	42
Figure 6-1 Line 1 Statistics	45
Figure 6-2 Line 1 Configuration	46
Figure 6-4 Line 1 Command Mode	48
Figure 6-6 Tunnel 1 Statistics	51
Figure 6-7 Tunnel 1 Serial Settings	52
Figure 6-9 Tunnel 1 Packing Mode (Mode = Disable)	53
Figure 6-10 Tunnel 1 Packing Mode (Mode = Timeout)	54
Figure 6-11 Tunnel 1 Packing Mode (Mode = Send Character)	54
Figure 6-13 Tunnel 1 Accept Mode	56
Figure 6-15 Tunnel 1 - Connect	59
Figure 6-17 Host 1, Host 2, Host 3 Exchanged	62
Figure 6-18 Tunnel 1 Disconnect Mode	63
Figure 6-21 Tunnel 1 Modem Emulation	65
Figure 7-1 Terminal on Line Configuration	67
Figure 7-3 Terminal on Network Configuration	69
Figure 7-5 Host Configuration	70

Figure 8-1 CPM: CPs	72
Figure 8-4 CPM: Groups	74
Figure 8-6 CPM: Group Status	75
Figure 9-1 DNS Settings	78
Figure 9-2 PPP Configuration Settings	80
Figure 9-4 SNMP Configuration	81
Figure 9-6 FTP Configuration	83
Figure 9-8 TFTP Configuration	84
Figure 9-10 Syslog	85
Figure 9-12 HTTP Statistics	86
Figure 9-13 HTTP Configuration	87
Figure 9-15 HTTP Authentication	89
Figure 9-17 RSS	91
Figure 9-19 LPD Statistics	92
Figure 9-20 LPD Configuration	93
Figure 10-1 SSH Server: Host Keys (Upload Keys)	96
Figure 10-3 SSH Server: Host Keys (Upload Keys)	98
Figure 10-5 SSH Server: Host Keys (Create New Keys)	99
Figure 10-7 SSH Server: Authorized Users	101
Figure 10-9 SSH Client: Known Hosts	102
Figure 10-11 SSH Client: Users	103
Figure 10-14 SSL	108
Figure 11-5 Modbus Statistics	114
Figure 11-6 Modbus Configuration	115
Figure 12-1 Filesystem Statistics	116
Figure 12-2 Filesystem Browser	117
Figure 12-4 TCP Protocol	119
Figure 12-6 IP Protocol	120
Figure 12-8 ICMP Protocol	121
Figure 12-10 ARP Protocol Page	122
Figure 12-12 SMTP	123
Figure 12-14 IP Address Filter Configuration	124
Figure 12-16 Query Port Configuration	125
Figure 12-17 Diagnostics: Hardware	126
Figure 12-18 MIB-II Network Statistics	127
Figure 12-20 IP Sockets	128
Figure 12-21 Diagnostics: Ping	129
Figure 12-23 Diagnostics: Traceroute	130

Figure 12-25 Diagnostics: Log	130
Figure 12-26 Diagnostics: Log (Filesystem)	131
Figure 12-27 Diagnostics: Log (Line 1)	131
Figure 12-28 Verbosity Configuration	132
Figure 12-30 Diagnostics: Memory	133
Figure 12-31 Diagnostics: Buffer Pools	133
Figure 12-32 Diagnostics: Processes	134
Figure 12-33 System	135
Figure 13-1 Email Statistics	137
Figure 13-2 Email Configuration	138
Figure 13-4 CLI Statistics	140
Figure 13-5 CLI Configuration	141
Figure 13-7 XML: Export Configuration	143
Figure 13-9 XML: Export Status	144
Figure 13-11 XML: Import Configuration	145
Figure 13-12 XML: Import Configuration from External File	145
Figure 13-13 XML: Import from Filesystem	146
Figure 13-14 XML: Import Configuration from Filesystem	147
Figure 13-15 XML: Import Line(s) from Single Line Settings on the Filesystem	148
Figure 13-17 CPU Power Management	149
Figure 14-1 Bridge 1 (bridge0) Status	152
Figure 14-3 Bridge 1 (bridge0) Configuration	154
Figure 17-1 Update Firmware	159

1: About This Guide

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

Chapter and Appendix Summaries

A summary of each chapter is provided below.

Chapter	Description
Chapter 2: Introduction	Main features of the product and the protocols it supports. Includes technical specifications.
Chapter 3: Using DeviceInstaller	Instructions for viewing the current configuration using DeviceInstaller.
Chapter 4: Configuration Using Web Manager	Instructions for accessing Web Manager and using it to configure settings for the device.
Chapter 5: Network Settings	Instructions for using the web interface to configure Ethernet settings.
Chapter 6: Line and Tunnel Settings	Instructions for using the web interface to configure line and tunnel settings.
Chapter 7: Terminal and Host Settings	Instructions for using the web interface to configure terminal and host settings.
Chapter 8: Configurable Pin Manager	Information about the Configurable Pin Manager (CPM) and how to set the configurable pins to work with a device.
Chapter 9: Service Settings	Instructions for using the web interface to configure settings for DNS, SNMP, FTP, and other services.
Chapter 10: Security Settings	Instructions for using the web interface to configure SSH and SSL security settings.
Chapter 11: Modbus	Instructions for using the web interface to configure Modbus.
Chapter 12: Maintenance and Diagnostics Settings	Instructions for using the web interface to maintain the device, view statistics, files, and logs, and diagnose problems.
Chapter 13: Advanced Settings	Instructions for using the web interface to configure email, CLI, and XML settings.
Chapter 14: Bridging	Information for configuring and using Bridging.
Chapter 15: Security in Detail	Provides additional information on security settings available.
Chapter 16: Branding the MatchPort b/g Pro	Instructions for customizing the device.
Chapter 17: Updating Firmware	Instructions for obtaining the latest firmware and updating the device.
Appendix A: Technical Support	Instructions for contacting Lantronix Technical Support.
Appendix B: Compliance	Lantronix compliance information.
Appendix C: Binary to Hexadecimal Conversions	Instructions for converting binary values to hexadecimals.
Appendix D: Warranty	Provides link to Lantronix warranty policy online.

Additional Documentation

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

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

2: *Introduction*

This chapter introduces the Lantronix MatchPort® b/g Pro 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 b/g Pro embedded Wireless 802.11 Device Server is a complete network-enabling solution on a 1.75"x1.75" PCB. This miniature device server empowers original equipment manufacturers (OEMs) to go to market quickly and easily with wireless 802.11 networking and web page serving capabilities built into their products.

This chapter contains the following sections:

- ◆ *Key Features*
- ◆ *Applications*
- ◆ *Protocol Support*
- ◆ *Evolution OS*
- ◆ *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:** 8 MB Flash and 8 MB SDRAM.
- ◆ **Wireless:** IEEE 802.11 b/g radio fully compliant with 802.11i security specifications.
- ◆ **Ethernet:** Optional 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 +70°C.

Applications

The MatchPort b/g Pro embedded device server connects serial devices such as those listed below to Ethernet or Wireless LAN (WLAN) networks using the IP protocol family.

- ◆ Medical devices
- ◆ ATM machines
- ◆ POS equipment
- ◆ Telecommunications equipment
- ◆ Security alarms and access control devices
- ◆ Handheld instruments
- ◆ Time/attendance clocks and terminals

Protocol Support

The MatchPort b/g Pro 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 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.
- ◆ IEEE802.11bg, WPA, WPA2/IEEE802.11i, IEEE802.1X, Personal (PSK), Enterprise (EAP-TLS, EAP-TTLS, PEAP, LEAP) for wireless connectivity.

Evolution OS

The MatchPort b/g Pro incorporates the Lantronix Evolution OS® operating system. Key features of the Evolution OS include:

- ◆ Built-in Web server for configuration and troubleshooting from Web-based browsers
- ◆ CLI configurability
- ◆ Wireless Interface (802.11 b/g) with WEP, WPA, IEEE 802.11i (WPA2-Personal, WPA2-Enterprise) protection.
- ◆ SNMP management
- ◆ XML data transport and configurability
- ◆ Really Simple Syndication (RSS) information feeds
- ◆ Enterprise-grade security with SSL and SSH
- ◆ Comprehensive troubleshooting tools

Additional Features

Modem Emulation

In modem emulation mode, the MatchPort b/g Pro 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 b/g Pro 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 b/g Pro with the Evolution OS uses industry-standard tools for configuration, communication, and control. For example, the Evolution OS uses a Command Line Interface (CLI) whose syntax is very similar to that used by data center equipment such as routers and hubs.

SNMP Management

The MatchPort b/g Pro 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 b/g Pro device servers.

XML-Based Architecture and Device Control

XML is a fundamental building block for the future growth of M2M networks. The MatchPort b/g Pro 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 b/g Pro 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 b/g Pro 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 b/g Pro 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 b/g Pro cannot be used to bring down other devices on the network.

You can use the MatchPort b/g Pro 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 b/g Pro 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, connections to the console ports of the attached devices as well as network hosts, such as Unix servers or another MatchPort, 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 b/g Pro 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 b/g Pro, including CPU utilization and total stack space available.

Configuration Methods

After installation, the MatchPort b/g Pro 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 b/g Pro 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 b/g Pro settings using the Lantronix Web Manager. See [Configuration Using Web Manager \(on page 23\)](#).

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 b/g Pro Embedded Device Server Command Reference* for instructions and available commands.)

XML: The MatchPort b/g Pro 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 b/g Pro 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.

Figure 2-1 Sample Hardware Address
00-20-4A-14-01-18 **or** 00:20:4A:14:01:18

IP Address

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

Port Numbers

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

The following is a list of the default server port numbers running on the MatchPort b/g Pro:

- 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

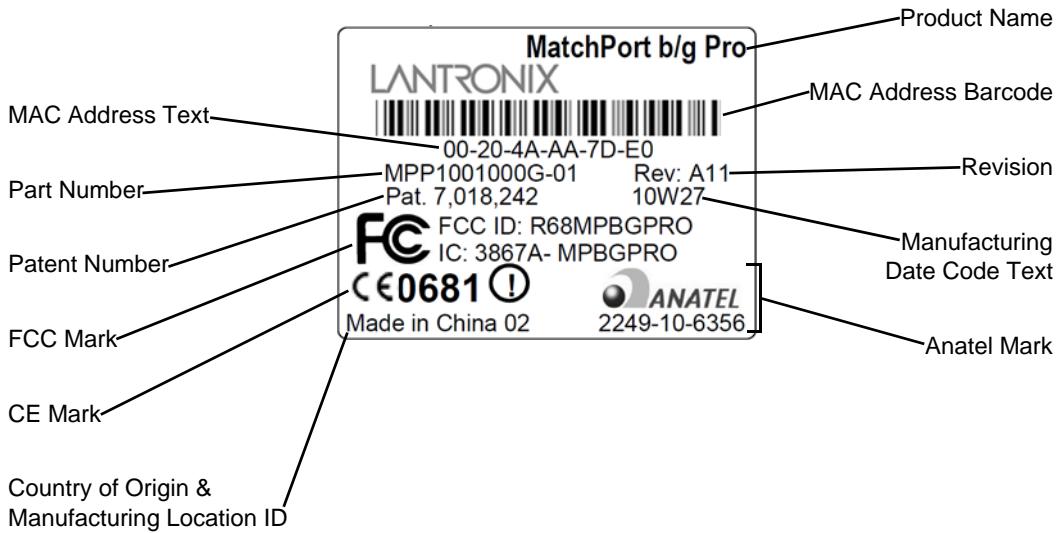
Note: Multi-port products include one or more additional supported ports and tunnels with default sequential numbering. For instance: TCP/UDP Port 10002: Tunnel 2, TCP/UDP Port 10003: Tunnel 3, etc.

Product Information Label

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

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

Figure 2-2 Product Label



3: Using DeviceInstaller

This chapter covers the steps for locating a device and viewing its properties and details. DeviceInstaller™ is a free utility program provided by Lantronix® that discovers, configures, upgrades and manages Lantronix device servers. It can be downloaded from the Lantronix website at www.lantronix.com/support/downloads.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 b/g Pro Using DeviceInstaller

Note: Make note of the MAC address. It is needed to locate the MatchPort® b/g Pro 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 b/g Pro 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 b/g Pro 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 3-1 Device Details Summary

Current Settings	Description
Name	Name identifying the MatchPort b/g Pro.
DHCP Device Name	Shows the name associated with the MatchPort b/g Pro' current IP address, if the IP address was obtained dynamically.
Group	Configurable field. Enter a group to categorize the MatchPort b/g Pro. 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.

Current Settings (continued)	Description
Comments	Configurable field. Enter comments for the MatchPort b/g Pro. 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.
Device Family	Shows the MatchPort b/g Pro device family type as “”.
Short Name	Shows “matchport_bg_pro” by default.
Long Name	Shows “Lantronix MatchPort b/g Pro” by default.
Type	Shows the specific device type, such as “MatchPort b/g Pro”.
ID	Shows the MatchPort b/g Pro ID embedded within the unit.
Hardware Address	Shows the MatchPort b/g Pro hardware (MAC) address.
Firmware Version	Shows the firmware currently installed on the MatchPort b/g Pro.
Extended Firmware Version	Provides additional information on the firmware version.
Online Status	Shows the MatchPort b/g Pro status as Online, Offline, Unreachable (the MatchPort b/g Pro is on a different subnet), or Busy (the MatchPort b/g Pro is currently performing a task).
IP Address	Shows the MatchPort b/g Pro current IP address. To change the IP address, click the Assign IP button on the DeviceInstaller menu bar.
IP Address was Obtained	Displays “Dynamically” if the MatchPort b/g Pro automatically received an IP address (e.g., from DHCP). Displays “Statically” if the IP address was configured manually. If the IP address was assigned dynamically, the following fields appear: <ul style="list-style-type: none">◆ 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 b/g Pro 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 b/g Pro.
Supports Configurable Pins	Shows , indicating configurable pins are available on the MatchPort b/g Pro.
Supports Email Triggers	Shows True, indicating email triggers are available on the MatchPort b/g Pro.
Telnet Supported	Indicates whether Telnet is enabled on this MatchPort b/g Pro.
Telnet Port	Shows the MatchPort b/g Pro port for Telnet sessions.
Web Port	Shows the MatchPort b/g Pro port for Web Manager configuration.
Firmware Upgradable	Shows True, indicating the MatchPort b/g Pro firmware is upgradable as newer versions become available.

4: Configuration Using Web Manager

This chapter describes how to configure the MatchPort® b/g Pro 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 b/g Pro in the address bar. The IP address may have been assigned manually using DeviceInstaller (see the *MatchPort Embedded Device Server Demonstration Kit Quick Start Guide*) or automatically by DHCP.

Figure 4-1 Prompt for User Name and Password



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

The screenshot shows the MatchPort b/g Pro Web Manager interface. On the left is a vertical navigation menu with various links such as Status, Bridge, CLI, CPM, CPU Power Mgmt, Diagnostics, DNS, Email, Filesystem, FTP, Host, HTTP, IP Address Filter, Line, LPD, Modbus, Network, PPP, Protocol Stack, Query Port, RSS, SNMP, SSH, SSL, Syslog, System, Terminal, TFTP, Tunnel, VIP, WLAN Profiles, and XML. The main content area is titled "Device Status" and contains two tables under "Product Information" and "Network Settings". The "Product Information" table includes fields like Product Type (Lantronix MatchPort b/g Pro), Firmware Version (5.2.0.3R2), Build Date (Aug 30 2012 20:05:45), Serial Number (07082437J6N2NI), Uptime (7 days 01:47:08), Permanent Config (Saved), and Region (United States). The "Network Settings" table includes fields like Interface (eth0), Link (Auto 10/100 Mbps Auto Half/Full (100 Mbps Full)), MAC Address (00:20:4a:aa:33:2e), Hostname (<None>), IP Address (172.19.212.42/16), Default Gateway (172.19.0.1), Domain (<None>), Primary DNS (172.19.1.1), Secondary DNS (<None>), MTU (1500), and VIP Conduit (Disabled). Below these tables is a "Line Settings" table with two entries for RS232 ports. At the bottom of the main content area is a copyright notice: "Copyright © Lantronix, Inc. 2007-2012. All rights reserved." In the top right corner, there is a "Logout" link.

Product Information	
Product Type:	Lantronix MatchPort b/g Pro
Firmware Version:	5.2.0.3R2
Build Date:	Aug 30 2012 (20:05:45)
Serial Number:	07082437J6N2NI
Uptime:	7 days 01:47:08
Permanent Config:	Saved
Region:	United States

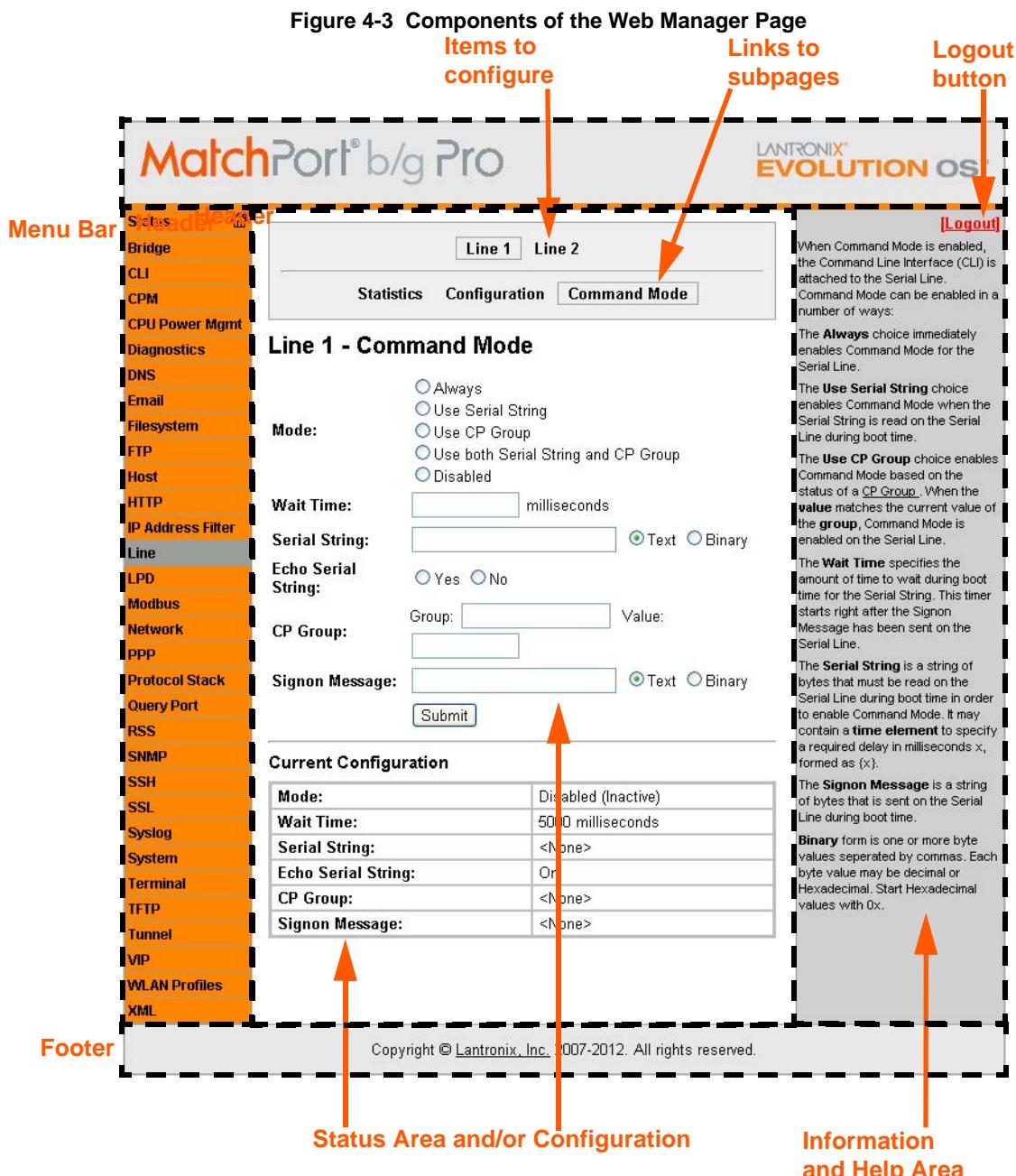
Network Settings	
Interface:	eth0
Link:	Auto 10/100 Mbps Auto Half/Full (100 Mbps Full)
MAC Address:	00:20:4a:aa:33:2e
Hostname:	<None>
IP Address:	172.19.212.42/16
Default Gateway:	172.19.0.1
Domain:	<None>
Primary DNS:	172.19.1.1
Secondary DNS:	<None>
MTU:	1500
VIP Conduit:	Disabled

Line Settings		
Line 1:	RS232, 9600, None, 8, 1, None	
Line 2:	RS232, 9600, None, 8, 1, None	
Tunneling	Connect Mode	Accept Mode
Tunnel 1:	Waiting	Waiting
Tunnel 2:	Disabled	Waiting

Copyright © Lantronix, Inc. 2007-2012. All rights reserved.

Web Manager Page Components

The layout of a typical Web Manager page is below.



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.
- 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 b/g Pro for the new configuration settings to take effect. The chapters that follow indicate when a change requires a reboot.*

Table 4-4 Summary of Web Manager Pages

Web Manager Page	Description	See Page
Status	Shows product information and network, line, and tunneling settings.	45
Bridge	Allows you to configure a bridge and shows the current operational state of the bridge.	150
CLI	Shows Command Line Interface (CLI) statistics and lets you change the current CLI configuration settings.	140
CPM	Shows information about the Configurable Pins Manager (CPM) and how to set the configurable pins and pin groups to work with a device.	71
CPU Power Management	Allows you to configure CPU power management, specifically the power management of the cpu, the on-chip peripherals and the extended memory.	149
Diagnostics	Lets you perform various diagnostic procedures.	126
DNS	Shows the current configuration of the DNS subsystem and the DNS cache.	78
Email	Shows email statistics and lets you clear the email log, configure email settings, and send an email.	137
Filesystem	Shows file system statistics and lets you browse the file system to view a file, create a file or directory, upload files using HTTP, copy a file, move a file, or perform TFTP actions.	116

Web Manager Page (continued)	Description	See Page
FTP	Shows statistics and lets you change the current configuration for the File Transfer Protocol (FTP) server.	82
Host	Lets you view and change settings for a host on the network.	69
HTTP	Shows HyperText Transfer Protocol (HTTP) statistics and lets you change the current configuration and authentication settings.	86
IP Address Filter	Lets you specify all the IP addresses and subnets that are allowed to send data to this device.	124
Line	Shows statistics and lets you change the current configuration and Command mode settings of a serial line.	45
LPD	Shows LPD (Line Printer Daemon) Queue statistics and lets you configure the LPD and print a test page.	92
Modbus	Shows the current connection status of the Modbus servers listening on the TCP ports and lets you configure the Modbus settings.	111
Network	Shows status and lets you configure the network interface.	28
PPP	Lets you configure a network link using Point-to-Point Protocol (PPP) over a serial line.	79
Protocol Stack	Lets you perform lower level network stack-specific activities.	119
Query Port	Lets you change configuration settings for the query port.	125
RSS	Lets you change current Really Simple Syndication (RSS) settings.	91
SNMP	Lets you change the current Simple Network Management Protocol (SNMP) configuration settings.	81
SSH	Lets you change the configuration settings for SSH server host keys, SSH server authorized users, SSH client known hosts, and SSH client users.	95
SSL	Lets you upload an existing certificate or create a new self-signed certificate.	105
Syslog	Lets you specify the severity of events to log and the server and ports to which the syslog should be sent.	84
System	Lets you reboot device, restore factory defaults, upload new firmware, and change the device long and short names.	135
Terminal	Lets you change current settings for a terminal.	67
TFTP	Shows statistics and lets you change the current configuration for the Trivial File Transfer Protocol (TFTP) server.	83
Tunnel	Lets you change the current configuration settings for a tunnel.	49
WLAN Profiles	Lets you view, edit, delete and create a WLAN profile on a device.	38
XML	Lets you export XML configuration and status records, and import XML configuration records.	142

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

Network 1		Network 2
Interface		Link
Status	Configuration	
Network 1 (eth0) Interface Status		
	Current	After Reboot
State:	Enabled	Enabled
BOOTP Client:	Off	Off
DHCP Client:	Off	Off
IP Address:	172.19.212.42	172.19.212.42
Network Mask:	255.255.0.0	255.255.0.0
Default Gateway:	172.19.0.1	172.19.0.1
Hostname:	<None>	<None>
Domain:	<None>	<None>
DNS Suffix Search List:		<None>
DHCP Client ID:	<None>	<None>
MTU:	1500	1500

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.

Figure 5-2 Network 1 (eth0) Interface Configuration

State:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
BOOTP Client:	<input type="radio"/> On <input checked="" type="radio"/> Off
DHCP Client:	<input type="radio"/> On <input checked="" type="radio"/> Off
IP Address:	172.19.212.42/16
Default Gateway:	172.19.0.1
Hostname:	
Domain:	
DHCP Client ID:	
	<input checked="" type="radio"/> Text <input type="radio"/> Binary
Primary DNS:	172.19.1.1
Secondary DNS:	<None>
MTU:	1500

2. Enter or modify the following settings:

Table 5-3 Network 1 (eth0) Interface Configuration

Network 1 Interface Configuration Settings	Description
State	Click to enable or disable the network interface: ◆ Enabled ◆ Disabled

Network 1 Interface Configuration Settings (continued)	Description
BOOTP Client	Select On or Off . At boot up, the device will attempt to obtain an IP address from a BOOTP server. Notes: <ul style="list-style-type: none"> ◆ 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.
DHCP Client	Select On or Off . At boot up, the device will attempt to lease an IP address from a DHCP server and maintain the lease at regular intervals. Note: Overrides BOOTP, the configured IP address, network mask, gateway, hostname, and domain.
IP Address	Enter the 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 Off . Changing this value requires you to reboot the device. Note: 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.
Default Gateway	Enter the IP address of the router for this network. Or, clear the field (appears as <None>). This address is only used for static IP address configuration.
Hostname	Enter the 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.
Domain	Enter the device domain name.
DHCP Client ID	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. Note: "Binary" entry mode allows a mixed mode of text and special characters in brackets. For example, "abcd<ctrl>A" would be entered "abcd[0x01]".
Primary DNS	IP address of the primary name server. This entry is required if you choose to configure DNS (Domain Name Server) servers.
Secondary DNS	IP address of the secondary name server.
MTU	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.

- 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

Status	
Speed:	100 Mbps
Duplex:	Full

Configuration	
Speed:	<input checked="" type="radio"/> Auto <input type="radio"/> 10Mbps <input type="radio"/> 100Mbps
Duplex:	<input checked="" type="radio"/> Auto <input type="radio"/> Half

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

Network 1-Ethernet Link Settings	Description
Speed	Select the Ethernet link speed. Default is Auto .
Duplex	Select the Ethernet link duplex mode. Default is Auto .

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.

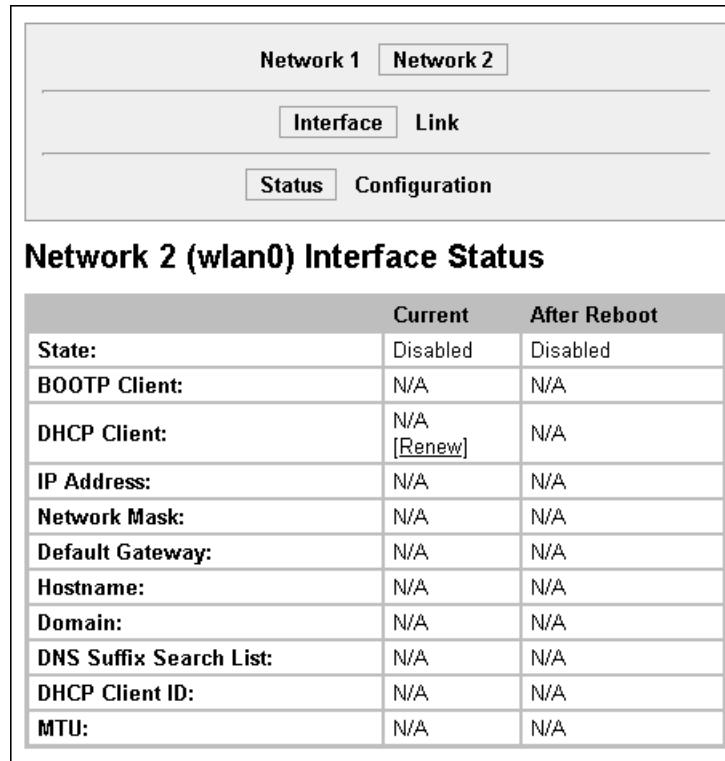
Network 2 (wlan0) Interface Status

This page shows the status of the wireless network interface.

To view the network interface status:

Click **Network** on the menu then click **Network 2 > Interface > Status** at the top of the page. The Network 2 (wlan0) Interface Status page appears.

Figure 5-6 Network 2 (wlan0) Interface Status



The screenshot shows a web-based interface for viewing network status. At the top, there are tabs for "Network 1" and "Network 2", with "Network 2" being active. Below that are tabs for "Interface" and "Link", with "Interface" being active. At the bottom are tabs for "Status" and "Configuration", with "Status" being active. The main content area is titled "Network 2 (wlan0) Interface Status" and contains a table with the following data:

	Current	After Reboot
State:	Disabled	Disabled
BOOTP Client:	N/A	N/A
DHCP Client:	N/A [Renew]	N/A
IP Address:	N/A	N/A
Network Mask:	N/A	N/A
Default Gateway:	N/A	N/A
Hostname:	N/A	N/A
Domain:	N/A	N/A
DNS Suffix Search List:	N/A	N/A
DHCP Client ID:	N/A	N/A
MTU:	N/A	N/A

Network 2 (wlan0) 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 2 (wlan0) Interface Configuration page appears.

Figure 5-7 Network 2 (wlan0) Interface Configuration

Network 2 (wlan0) Interface Configuration	
State:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
BOOTP Client:	<input type="radio"/> On <input checked="" type="radio"/> Off
DHCP Client:	<input checked="" type="radio"/> On <input type="radio"/> Off
IP Address:	<None>
Default Gateway:	<None>
Hostname:	
Domain:	
DHCP Client ID:	
	<input checked="" type="radio"/> Text <input type="radio"/> Binary
Primary DNS:	<None>
Secondary DNS:	<None>
MTU:	1500

2. Enter or modify the following settings:

Table 5-8 Network 2 (wlan0) Interface Configuration

Network 2 (wlan0) Interface Configuration Setting	Description
State	Click to enable or disable the network interface: ◆ Enabled ◆ Disabled
BOOTP Client	Select On or Off . At boot up, the device will attempt to obtain an IP address from a BOOTP server. Notes: <ul style="list-style-type: none"> ◆ 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.
DHCP Client	Select On or Off . At boot up, the device will attempt to lease an IP address from a DHCP server and maintain the lease at regular intervals. Note: Overrides BOOTP, the configured IP address, network mask, gateway, hostname, and domain.

Network 2 (wlan0) Interface Configuration (continued)	Description
IP Address	<p>Enter the device static IP address.</p> <p>You may enter it alone, in CIDR format, or with an explicit mask.</p> <p>The IP address consists of four octets separated by a period and is used if BOOTP and DHCP are both set to Off. Changing this value requires you to reboot the device.</p> <p>Note: 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.</p>
Default Gateway	Enter the IP address of the router for this network. Or, clear the field (appears as <None>). This address is only used for static IP address configuration.
Hostname	Enter the 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.
Domain	Enter the device domain name.
DHCP Client ID	<p>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.</p> <p>Note: "Binary" entry mode allows a mixed mode of text and special characters in brackets. For example, "abcd<ctrl>A" would be entered "abcd[0x01]".</p>
Primary DNS	IP address of the primary name server. This entry is required if you choose to configure DNS (Domain Name Server) servers.
Secondary DNS	IP address of the secondary name server.
MTU	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.

- Click **Submit** to save changes.

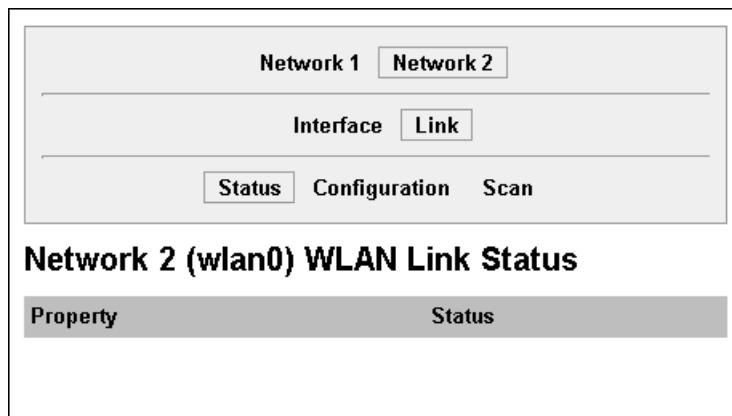
Network 2 (wlan0) WLAN Link Status

This page shows the status of the wireless link.

To view the WLAN Link Status:

Click **Network** on the menu then click **Network 2 > Link > Status** at the top of the page. The Network 2 (wlan0) WLAN Link Status page appears.

Figure 5-9 Network 2 (wlan0) WLAN Link Status



Network 2 (wlan0) WLAN Link Configuration

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

To view and configure wireless link settings:

1. Click **Network** on the menu bar and then **Network 2 > Link > Configuration** at the top of the page. The Network 2 (wlan0) WLAN Link Configuration page appears.

Figure 5-10 Network 2 (wlan0) WLAN Link Configuration

Choice 1 Profile:	default_infrastructure_profile
Choice 2 Profile:	default_adhoc_profile
Choice 3 Profile:	
Choice 4 Profile:	
Out of Range Scan Interval:	30 seconds
Roaming:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled

2. Enter or modify the following settings:

Table 5-11 Network 2 (wlan0) Interface Configuration

Network 2 (wlan0) WLAN Link Configuration Setting	Description
Choice 1 Profile	List the selected WLAN profiles in order of preference here. The order of preferences listing is referenced sequentially during Access Point (AP) roaming.
Choice 2 Profile	The configuration details are stored in one or more WLAN profile. Click Apply to try out the settings on the WLAN without saving them to Flash. If the settings do not work, the device will retain the original settings upon a reboot.
Choice 3 Profile	
Choice 4 Profile	
Out of Range Scan Interval	Set the amount of time in seconds, between AP roaming and association attempts. It is set to a default of 30 seconds.
Roaming	<p>Click to enable or disable wireless LAN roaming:</p> <ul style="list-style-type: none"> ◆ Enabled ◆ Disabled <p>Roaming will allow automatic association with a different Access Point (AP) possessing the same Network Name, if its signal strength is sufficiently stronger than the current AP association. A stronger signal is one which is 20 dBm greater than the current signal strength, if the current signal strength is equal to or greater than -40 dBm. A stronger signal need only be 10 dBm greater if the current signal strength is less than -40 dBm.</p> <p>If 802.11f (IEEE standard for AP interoperability) is supported by both the old AP and newly associated AP to which roaming has occurred, a short delay will occur as the routing table of each AP is updated. If, however, 802.11f is not supported the delay will be longer and may result in the termination of any active TCP/IP connections.</p>

3. Click Submit to save changes.

Network 2 (wlan0) WLAN Link Scan

This page is where a wireless link scan can be made of wireless devices within the range of the device. The scan reports the Network name, basic service set identifier (BSSID), channel number(CH), received signal strength indication (RSSI) and topology (T).

To view and configure wireless link settings:

1. Click **Network** on the menu bar and then **Network 2 > Link > Scan** at the top of the page. The Network 2 (wlan0) WLAN Link Configuration page appears.

Figure 5-12 Network 2 (wlan0) WLAN Link Scan

The screenshot shows a network management interface for Network 2 (wlan0). At the top, there are tabs for Network 1 and Network 2, with Network 2 selected. Below that are tabs for Interface, Link, Status, Configuration, and Scan, with Scan selected. The main area is titled "Network 2 (wlan0) WLAN Link Scan". A "Network name:" input field and a "Scan" button are present. The table below lists wireless networks:

Network name	BSSID	Ch	RSSI	Topology
	00:0b:85:1a:cc:6f	11	-84 dBm	I
	00:18:39:ba:fb:a4	11	-89 dBm	I
	00:0b:85:1a:c8:bd	1	-86 dBm	I
	00:0b:85:1a:cc:6d	11	-84 dBm	I
EVOTESTING	00:1d:7e:e7:d2:e9	10	-59 dBm	I
LTRX_IBSS	00:18:f6:55:d7:1a	6	-85 dBm	I
PATLAB_WPA2CCMPTKIP	00:1e:c1:ac:0f:62	2		I
RADIUSAUTH	00:12:01:58:7c:10	8	-85 dBm	I

- Enter or modify the following settings:

Table 5-13 Network 2 (wlan0) WLAN Link Scan

Network 2 (wlan0) WLAN Link Scan Setting	Description
Network name	Enter the network tname for a filtered response or leave it blank to see all networks.

- Click **Scan** for scan results. The following information appears about each wireless device within range.

Table 5-14 Device Information within Range

Network 2 WLAN Link Scan Page	Description
Network Name	Name of the wireless network (SSID).
BSSID	Basic Service Set Identifier.
Ch	Channel number.
RSSI	Received Signal Strength Indication.
Topology	Infrastructure or Adhoc.

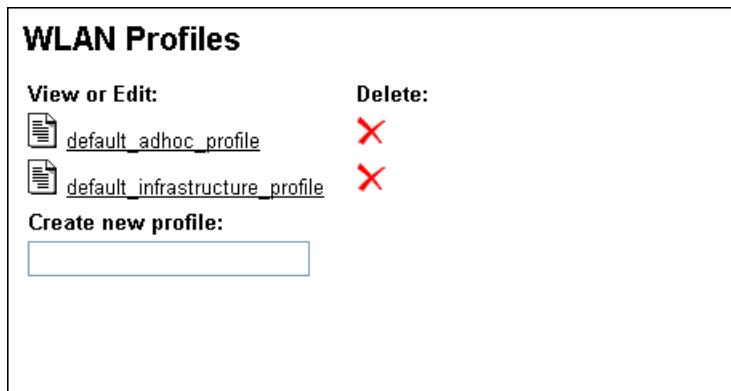
WLAN Profiles

This page allows you to view, edit, delete, or create a WLAN profile on the device.

To create, edit or delete a WLAN profile:

1. On the menu, click **WLAN Profiles**. The WLAN Profiles page appears with any existing WLAN profiles listed.

Figure 5-15 WLAN Profiles



2. **To delete an existing WLAN profile**, click the **X** to the right of the specific profile and **OK** in the resulting verification popup window. A message indicating that the profile is deleted appears on the screen.
3. **To create a new WLAN profile**, enter a name for the profile in the **Create new profile** field and click **Submit**. The new WLAN profile name appears in the list. Continue to the next step to configure the new profile.
4. **To view or edit an existing WLAN profile**, including newly created profiles, click the specific profile in the list. The WLAN Profile page ([Figure 5-16](#)) appears with the details of the selected profile.

Figure 5-16 WLAN Profile Page

WLAN Profile "default_adhoc_profile"

Basic Configuration	
Network Name (SSID):	Lantronix Initial Adhoc Network
Topology:	<input type="radio"/> Infrastructure <input checked="" type="radio"/> Adhoc
Channel:	1
Advanced Configuration	
Adhoc Merging:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
TX Data Rate Maximum:	54 Mbps
TX Data Rate:	<input type="radio"/> Fixed <input checked="" type="radio"/> Auto-reduction
TX Power Maximum:	14 dBm
TX Power:	<input type="radio"/> Fixed <input checked="" type="radio"/> Adaptation
TX Retries:	7
Power Management:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Security Configuration	
Suite:	None

5. Email or modify the following settings:

Table 5-17 WLAN Profile Page Settings

WLAN Profile Basic Page Settings	Description
Network Name	Enter the name of the wireless network (SSID).
Topology	Select Infrastructure (ESS) mode or Adhoc (IBSS) mode. <ul style="list-style-type: none"> ◆ Infrastructure: mode that communicates with access points. ◆ Adhoc: mode that communicates only with other clients. <p>Note: Your selection affects the settings displayed in this section and the Advanced section of this page.</p>
Channel	Enter the radio channel for the Adhoc network. <p>Note: This option only appears when Adhoc mode is selected.</p>
Adhoc Merging	Select to enable or disable Adhoc Merging: <ul style="list-style-type: none"> ◆ Enabled ◆ Disabled <p>Note: This option only appears when Adhoc mode is selected.</p>
TX Data Rate Maximum	Enter the maximum rate of data transmission. The default is 54 Mbps .
TX Data Rate	MatchPort b/g Pro lets you control the transmission data rate or controls it automatically. <ul style="list-style-type: none"> ◆ Fixed = keeps the transmission rate at the configured maximum. ◆ Auto-reduction = allows the MatchPort to reduce the data rate from the maximum automatically, depending on link quality.
TX Power Maximum	Maximum transmission output power in dBm.

WLAN Profile Basic Page Settings (continued)	Description
TX Power	Select the type of radio power control. <ul style="list-style-type: none"> ◆ Fixed = keeps the transmission output power at the configured maximum. ◆ Adaptation = allows the MatchPort to reduce the output power automatically when closer to the Access Point or peer client. This reduces power consumption and allows a higher density of clients in a given area.
TX Retries	Number of times the MatchPort will attempt to transmit data before the packet is deemed lost. <i>Note:</i> A value of '1' means 1 try with 0 retries.
Power Management	Power management reduces the overall power consumption of the MatchPort unit, but can increase latency. <ul style="list-style-type: none"> ◆ Enabled = allows the MatchPort to turn off the receiver when it is idling. ◆ Disabled = keeps the receiver on at all times.
Power Management Interval	Number of beacons (100 ms interval) between 1 and 10. The above-mentioned latency increase can be up to this number x 100 ms. <i>Note:</i> This field appears if Power Management is enabled.
Suite	Select one of the following types of security for the WLAN profile. They are listed in ascending order of degree of security: <ul style="list-style-type: none"> ◆ None = no authentication or encryption method will be used. ◆ WEP = Wired Equivalent Privacy ◆ WPA = WiFi Protected Access ◆ WPA2/IEEE 802.11i = Robust Secure Network <i>Note:</i> Depending on your choices for Suite, Key Type, Authentication, and IEEE 802.1x, different fields display. WPA and WPA2/IEEE 802.11i are not available for Adhoc topology. The WPA2/IEEE 802.11i mode is compliant with the Robust Secure Network specified in the IEEE standard 802.11i.

WEP Settings

WEP security is available in both **Infrastructure** and **AdHoc** modes. WEP is a simple and efficient security mode encrypting the data via the RC4 algorithm. However, WEP has become more vulnerable due to advances in hacking technology. State of the art equipment can find WEP keys in five minutes. For stronger security, please use WPA, or better, WPA2 with AES (CCMP).

Figure 5-18 WLAN Profile Security -- WEP Settings

Security Configuration	
Suite:	WEP
Authentication:	<input checked="" type="radio"/> Open <input type="radio"/> Shared
Key Type:	<input type="radio"/> Passphrase <input checked="" type="radio"/> Hex
Key Size:	<input checked="" type="radio"/> 40 bits <input type="radio"/> 104 bits
TX Key Index:	1
Key 1:	<None>
Key 2:	<None>
Key 3:	<None>
Key 4:	<None>

Table 5-19 WLAN Profile Security - WEP Settings

WLAN Profile Security Configuration WEP Settings	Description
Authentication	Select an authentication scheme from the drop-down list. <ul style="list-style-type: none"> ◆ Shared = encryption keys of both parties are compared as a form of authentication. If mismatched, no connection is established. ◆ Open = a connection is established without first checking for matching encryption keys. However, mismatched keys will result in garbled data and thus a lack of connectivity on the IP level.
Key Type	Select the format of the security key. <ul style="list-style-type: none"> ◆ Passphrase = A text of up to 63 characters converted to 4 encryption keys. ◆ Hex = 4 individually entered encryption keys consisting of hexadecimal digits.
Key Size	Key size in bits. Select 40 for WEP40 and WEP64, select 104 for WEP104 and WEP128.
TX Key Index	Select one of four indexes listing keys for transmitting data. Reception is allowed with all four keys. <p>Note: For operability with some products that generate four identical keys from a passphrase, this index must be one.</p>
Keys 1-4	Enter one or more encryption keys in hexadecimal format. Enter 10 hexadecimal digits (0-9, a-f) for WEP40 and 26 for WEP104. The configured keys are not shown for security reasons. <p>Note: This field only appears if Key Type is Hex.</p>

WPA and WPA2/IEEE802.11i Settings

WPA and WPA2/IEEE802.11i security suites are available for **Infrastructure** mode only. Since the configuration options are the same for both, they are described in one chapter. The settings that display depend on which **Authentication** method is selected, as shown in the figures below.

WPA is a security standard specified by the WiFi Alliance and is a close derivative of an early draft of the IEEE802.11i specification. WEP was becoming vulnerable and finalizing the IEEE802.11i standard was still far away. WPA2 is WiFi's subset of the broad IEEE802.11i standard to enforce better interoperability. The MatchPort b/g Pro is compliant with both WPA2 and IEEE802.11i.

Figure 5-20 WLAN Profile Security – WPA with PSK Authentication

Security Configuration	
Suite:	WPA
Authentication:	<input checked="" type="radio"/> PSK <input type="radio"/> IEEE 802.1X
Key Type:	<input type="radio"/> Passphrase <input checked="" type="radio"/> Hex
Key:	<None>
Encryption:	<input type="checkbox"/> CCMP <input type="checkbox"/> TKIP <input type="checkbox"/> WEP
Validate Certificate:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled

Figure 5-21 WLAN Profile Security – WPA2/IEEE 802.11i with PSK Authentication

Security Configuration	
Suite:	WPA2 / IEEE 802.11i
Authentication:	<input checked="" type="radio"/> PSK <input type="radio"/> IEEE 802.1X
Key Type:	<input checked="" type="radio"/> Passphrase <input type="radio"/> Hex
Passphrase:	<None>
Encryption:	<input type="checkbox"/> CCMP <input type="checkbox"/> TKIP <input type="checkbox"/> WEP
Validate Certificate:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled

Figure 5-22 WLAN Profile Security – WPA with IEEE 802.1X Authentication

Security Configuration	
Suite:	WPA
Authentication:	<input type="radio"/> PSK <input checked="" type="radio"/> IEEE 802.1X
IEEE 802.1X:	EAP-TTLS
EAP-TTLS Option:	EAP-MSCHAPV2
Username:	
Password:	<None>
Encryption:	<input type="checkbox"/> CCMP <input type="checkbox"/> TKIP <input type="checkbox"/> WEP
Validate Certificate:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled

Figure 5-23 WLAN Profile Security – WPA2/IEEE 802.11i with IEEE 802.1X Authentication

Security Configuration	
Suite:	WPA2 / IEEE 802.11i
Authentication:	<input type="radio"/> PSK <input checked="" type="radio"/> IEEE 802.1X
IEEE 802.1X:	EAP-TTLS
EAP-TTLS Option:	EAP-MSCHAPV2
Username:	
Password:	<None>
Encryption:	<input type="checkbox"/> CCMP <input type="checkbox"/> TKIP <input type="checkbox"/> WEP
Validate Certificate:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled

Table 5-24 WPA and WPA2/IEEE802.11i Settings

WLAN Profile Security WPA & WPA2 Settings	Description
Authentication	Select an authentication scheme. <ul style="list-style-type: none"> ◆ PSK = Pre-Shared Key. The same key needs to be configured on both sides of the connection. (On the MatchPort b/g Pro and on the Access Point.) ◆ IEEE 802.1X = This authentication method communicates with a Radius authentication server that is part of the network. The Radius server will match the credentials sent by the MatchPort b/g Pro with an internal database.
Key Type	Select the format of the security key. <ul style="list-style-type: none"> ◆ Passphrase ◆ Hex <p>Note: This field only appears if authentication is PSK.</p>
Key	64 hexadecimal digits. <p>Note: This field only appears if Key Type is Hex.</p>
Passphrase	The passphrase consists of text of up to 63 characters and is hashed into a 32 byte encryption key using a repeated SHA1 algorithm. <p>Note: Lantronix recommends using a passphrase of 20 characters or more for maximum security. Spaces and punctuation characters are permitted. The passphrase input is not the same as ASCII input (as used on some products). ASCII is translated directly into hexadecimal bytes according to the ASCII table, while a possibly larger passphrase is hashed into a key and provides better security through a larger range of key values. This field only appears if Key Type is Passphrase.</p>
IEEE 802.1X	From the drop-down list, select the protocol to use to authenticate the WLAN client. <ul style="list-style-type: none"> ◆ LEAP = Lightweight Extensible Authentication Protocol. ◆ A derivative of the original Cisco LEAP, which was a predecessor of 802.1X. Real Cisco LEAP uses a special MAC layer authentication (called Network EAP) and cannot work with WPA/WPA2. The MatchPort b/g Pro uses a more generic version to be compatible with other major brand WiFi equipment. The authentication backend is the same. ◆ EAP-TLS = Extensible Authentication Protocol - Transport Layer Security. ◆ Uses the latest incarnation of the Secure Sockets Layer (SSL) standard and is the most secure because it requires authentication certificates on both the network side and the MatchPort b/g Pro side. ◆ EAP-TTLS = Extensible Authentication Protocol - Tunneled Transport Layer Security. ◆ PEAP = Protected Extensible Authentication Protocol. ◆ EAP-TTLS and PEAP have been developed to avoid the requirement of certificates on the client side (MatchPort b/g Pro), which makes deployment more cumbersome. Both make use of EAP-TLS to authenticate the server (network) side and establish an encrypted tunnel. This is called the outer-authentication. Then a conventional authentication method (MD5, MSCHAP, etc.) is used through the tunnel to authenticate the MatchPort b/g Pro. This is called inner authentication. ◆ EAP-TTLS and PEAP have been developed by different consortia and vary in details, of which the most visible is the supported list of inner authentications. <p>Note: When using EAP-TLS, EAP-TTLS or PEAP authority, at least one authority certificate will have to be installed in the SSL configuration that is able to verify the Radius server's certificate. In case of EAP-TLS, also a certificate and matching private key need to be configured to authenticate the MatchPort b/g Pro to the Radius server. This field only appears if authentication is IEEE802.1X. For more information about SSL certificates see SSL Settings on page 105.</p>

WLAN Profile Security WPA & WPA2 Settings (continued)	Description
EAP-TTLS Option	From the drop-down list, select the inner authentication. <ul style="list-style-type: none"> ◆ EAP-MSCHAPv2 ◆ MSCHAPv2 ◆ MSCHAP ◆ CHAP ◆ PAP ◆ EAP-MD5 <p>Note: This field only appears if IEEE802.1X is EAP-TTLS.</p>
PEAP Option	From the drop-down list, select the inner authentication. <ul style="list-style-type: none"> ◆ EAP-MSCHAPv2 ◆ EAP-MD5 <p>Note: This field only appears if IEEE802.X is PEAP.</p>
Username	Userid for identifying the MatchPort b/g Pro to the Radius server in the network. <p>Note: This option does not display for EAP-TLS. This field only appears if authentication is IEEE802.1X.</p>
Password	Password for identifying the MatchPort b/g Pro to the Radius server in the network. <p>Note: This option does not display for EAP-TLS. This field only appears if authentication is IEEE802.1X.</p>
Encryption	Select one or more encryption types, listed from strongest to least strong. At least one selection will have to match the Access Points intended to connect with. <ul style="list-style-type: none"> ◆ CCMP = Uses AES as basis and is the strongest encryption option. ◆ TKIP = Uses WEP as the basis, but adds extra checks and variations for added protection. ◆ WEP = Based on RC4. <p>Note: In case the encryption settings on the Access Point(s) can still be chosen, the capabilities of the Access Point(s) and the other clients that need to use the network need to be taken into account.</p>

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 embedded device server, 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 Modbus b/g Pro 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

Line 1	Line 2	Line 3	Line 4
Statistics	Configuration	Command Mode	
Line 1 - Statistics			
Line 1 - Statistics			
	Receiver	Transmitter	
Bytes:	0	0	
Breaks:	0	0	
Flow control:	N/A	N/A	
Parity Errors:	0		
Framing Errors:	0		
Overrun Errors:	0		
No Rx Buffer Errors:	0		
Queued Receive Bytes:	0		
Queued Transmit Bytes:	0		
CTS input:	not asserted		
RTS output:	asserted		
DSR input:	not asserted		
DTR output:	not asserted		

Line Configuration

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

The screenshot shows the Line 1 Configuration page with Line 2 selected. The top navigation bar includes tabs for Line 1 and Line 2, Statistics, Configuration (which is selected), and Command Mode. The main section is titled "Line 2 - Configuration" and contains a table with the following data:

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

-
4. Enter or modify the following settings:

Table 6-3 Line Configuration

Line - Configuration Settings	Description
Name	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 67 for related configuration information.
Interface	Select the interface type from the drop-down menu. The default is RS232.
State	Indicates whether the current line is enabled. To change the status, select Enabled or Disabled from the drop-down menu.
Protocol	Select the protocol from the drop-down menu. The default is Tunnel.
Baud Rate	Select the baud rate from the drop-down menu. The default is 9600.
Parity	Select the parity from the drop-down menu. The default is None.
Data Bits	Select the number of data bits from the drop-down menu. The default is 8.
Stop Bits	Select the number of stop bits from the drop-down menu. The default is 1.
Flow Control	Select the flow control from the drop-down menu. The default is None.
Xon Char	Specify the character to use to start the flow of data when Flow Control is set to Software. Prefix a decimal character with \ or a hexadecimal character with 0x, or provide a single printable character. The default Xon char is 0x11.
Xoff Char	Specify the character to use to stop the flow of data when Flow Control is set to Software. Prefix a decimal character with \ or a hexadecimal character with 0x, or provide a single printable character. The default Xoff char is 0x13.
Gap Timer	The driver forwards received serial bytes after the Gap Timer delay from the last character received. By default, the delay is four character periods at the current baud rate (minimum 1 ms).
Threshold	The driver will also forward received characters after Threshold bytes have been received.

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 Modbus b/g Pro 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.

Figure 6-4 Line 1 Command Mode

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

4. Enter or modify the following settings:

Table 6-5 Line Command Mode

Line – Command Mode Settings	Description
Mode	Select the method of enabling Command Mode or choose to disable Command Mode. <ul style="list-style-type: none"> ◆ 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.

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

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 b/g Pro, XPort AR, EDS8/16PS and EDS8/16/32PR) 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 \(on page 23\)](#) or the MatchPort b/g Pro Command Reference for the full list of commands.

The MatchPort b/g Pro 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 b/g Pro 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 b/g Pro 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 b/g Pro 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 b/g Pro logs statistics for tunneling. The Dropped statistic shows connections ended by the remote location. The Disconnects statistic shows connections ended by the MatchPort b/g Pro.

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

Tunnel 1	Tunnel 2	Tunnel 3	Tunnel 4
Statistics	Serial Settings	Packing Mode	
Accept Mode	Connect Mode	Disconnect Mode	
	Modem Emulation		

Tunnel 1 - Statistics

Aggregate Counters	
Completed Accepts:	0
Completed Connects:	0
Disconnects:	0
Dropped Accepts:	0
Dropped Connects:	0
Octets forwarded from Serial:	0
Octets forwarded from Network:	0
Accept Connection Time:	0 days 00:00:00
Connect 1 Connection Time:	0 days 00:00:00
Connect 2 Connection Time:	0 days 00:00:00
Connect 3 Connection Time:	0 days 00:00:00
Connect 4 Connection Time:	0 days 00:00:00
Connect 5 Connection Time:	0 days 00:00:00
Connect 6 Connection Time:	0 days 00:00:00
Connect 7 Connection Time:	0 days 00:00:00
Connect 8 Connection Time:	0 days 00:00:00
Connect DNS Address Changes:	0
Connect DNS Address Invalids:	0
Accept Counters	
There is no active connection.	
Connect 1 Counters	Kill Connection(s)
There is no active connection.	
Connect 2 Counters	
There is no active connection.	
Connect 3 Counters	
There is no active connection.	
Connect 4 Counters	
There is no active connection.	
Connect 5 Counters	
There is no active connection.	
Connect 6 Counters	
There is no active connection.	
Connect 7 Counters	
There is no active connection.	
Connect 8 Counters	
There is no active connection.	

Note: Tunnels 3 and 4 do not apply for Modbus b/g Pro 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

Line Settings:	RS232, 9600, None, 8, 1, None
Protocol:	Tunnel
DTR:	<input type="radio"/> Unasserted <input type="radio"/> TruPort <input checked="" type="radio"/> Asserted while connected <input type="radio"/> Continuously asserted

Note: Tunnels 3 and 4 do not apply for Modbus b/g Pro embedded device server.

4. View or modify the following settings:

Table 6-8 Tunnel - Serial Settings

Tunnel - Serial Settings	Description
Line Settings (display only)	Current serial settings for the line.
Protocol (display only)	The protocol being used on the line. In this case, Tunnel.

Tunnel - Serial Settings	Description
DTR	Select when to assert DTR. <ul style="list-style-type: none"> ◆ 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.

5. Click **Submit**.
6. 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.

Figure 6-9 Tunnel 1 Packing Mode (Mode = Disable)

Note: Tunnels 3 and 4 do not apply for Modbus b/g Pro embedded device server.

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: Tunnels 3 and 4 do not apply for Modbus b/g Pro embedded device server for Figure 6-10 and Figure 6-11.

Figure 6-10 Tunnel 1 Packing Mode (Mode = Timeout)

Tunnel 1	Tunnel 2	Tunnel 3	Tunnel 4
Statistics	Serial Settings	Packing Mode	
Accept Mode	Connect Mode	Disconnect Mode	
Modem Emulation			
Tunnel 1 - Packing Mode			
Mode:	<input type="radio"/> Disable <input checked="" type="radio"/> Timeout <input type="radio"/> Send Character		
Threshold:	512	bytes	
Timeout:	1000	milliseconds	
<input type="button" value="Submit"/>			

Figure 6-11 Tunnel 1 Packing Mode (Mode = Send Character)

Tunnel 1	Tunnel 2	Tunnel 3	Tunnel 4
Statistics	Serial Settings	Packing Mode	
Accept Mode	Connect Mode	Disconnect Mode	
Modem Emulation			
Tunnel 1 - Packing Mode			
Mode:	<input type="radio"/> Disable <input type="radio"/> Timeout <input checked="" type="radio"/> Send Character		
Threshold:	512	bytes	
Send Character:	<control>M		
Trailing Character:	<None>		
<input type="button" value="Submit"/>			

- Enter or modify the following settings:

Table 6-12 Tunnel Packing Mode

Tunnel - Packing Mode Settings	Description
Mode	<ul style="list-style-type: none"> ◆ 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 b/g Pro 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 b/g Pro 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 b/g Pro 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

Tunnel 2 - Accept Mode	
Mode:	Always
Local Port:	10002
Protocol:	TCP
TCP Keep Alive:	45000 milliseconds
Flush Serial:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Block Serial:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Block Network:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Password:	<None>
Email on Connect:	<None>
Email on Disconnect:	<None>
CP Output:	Group:

4. Enter or modify the following settings:

Table 6-14 Tunnel Accept Mode

Tunnel - Accept Mode Settings	Description
Mode	Select the method used to start a tunnel in Accept mode. Choices are: <ul style="list-style-type: none"> ◆ Disabled = do not accept an incoming connection. ◆ Always = accept an incoming connection (<i>default</i>) ◆ Any Character = start waiting for an incoming connection when any character is read on the serial line. ◆ Start Character = start waiting for an incoming connection when the start character for the specific tunnel is read on the serial line. ◆ Modem Control Asserted = start waiting for an incoming connection as long as the Modem Control pin (DSR) is asserted on the serial line until a connection is made. ◆ Modem Emulation = start waiting for an incoming connection when triggered by modem emulation AT commands. Connect mode must also be set to Modem Emulation.
Local Port	Enter the port number for use as the local port. The defaults are port 10001 for Tunnel 1. Additional tunnels, if supported, increase sequentially.
Protocol	Select the protocol type for use with Accept Mode. The default protocol is TCP. If you select TCP AES you will need to configure the AES keys.
TCP Keep Alive	Enter the time, in seconds, the 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.
Flush Serial Data	Select Enabled to flush the serial data buffer on a new connection.
Block Serial Data	Select On to block, or not tunnel, serial data transmitted to the device.
Block Network	Select On to block, or not tunnel, network data transmitted to the device.
Password	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.
Email on Connect	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.
Email on Disconnect	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.
CP Output	Identifies a CP or CP Group whose value should change when a connection is established and dropped. <ul style="list-style-type: none"> ◆ 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.

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

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 b/g Pro device will make a connection only if it can resolve the address. For DNS names, the MatchPort b/g Pro 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 MatchPort b/g Pro is the SSH client. Ensure the MatchPort b/g Pro SSH client username is configured on the remote SSH server before using it with the MatchPort b/g Pro.

- ◆ **SSL**
- ◆ **UDP**

Is only available in Connect Mode because it is a connectionless protocol. For Connect Mode using UDP, the MatchPort b/g Pro 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 b/g Pro 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 b/g Pro 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

Tunnel 2 - Connect Mode	
Mode:	Disable
Local Port:	<Random>
Host 1:	<None>
Reconnect Timer:	15000 milliseconds
Flush Serial Data:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Block Serial:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Block Network:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Email on Connect:	<None>
Email on Disconnect:	<None>
CP Output:	Group:

4. Enter or modify the following settings:

Table 6-16 Tunnel Connect Mode

Tunnel – Connect Mode Settings	Description
Mode	Select the method to be used to attempt a connection to a remote host or device. Choices are: <ul style="list-style-type: none"> ◆ Always = a connection is attempted until one is made. If the connection gets disconnected, the MatchPort b/g Pro retries until it makes a connection. (default) ◆ Disable = an outgoing connection is never attempted. ◆ Any Character = a connection is attempted when any character is read on the serial line. ◆ Start Character = a connection is attempted when the start character for the specific tunnel is read on the serial line. ◆ Modem Control Asserted = a connection is attempted as long as the Modem Control pin (DSR) is asserted, until a connection is made. ◆ Modem Emulation = a connection is attempted when triggered by modem emulation AT commands.
Local Port	Enter the port for use as the local port. A random port is selected by default. Once you have configured a number, click the Random link in the Current Configuration to switch back to random.
Host <i>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.</i>	Click <None> in the Host field to configure the Host parameters. <ul style="list-style-type: none"> ◆ Address = 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. ◆ Port = Enter the port for use as the Host Port. It designates the port on the remote host to connect to. Displays configured Port. ◆ Protocol = 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: <ul style="list-style-type: none"> ➢ For SSH, also enter an SSH Username. ➢ For SSL, also select Enabled or Disabled for Validate Certificate. ➢ For SSL, TCP, TCP AES and Telnet, use the TCP Keep Alive field to adjust the value. ➢ For TCP AES, enter the AES Encrypt and AES Decrypt Keys. Both of keys may be set to the same value. ➢ For UDP, 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. ➢ For UDP AES, enter the AES Encrypt and AES Decrypt Keys. ◆ SSH Username = Displays configured username, used only if SSH protocol is selected. ◆ TCP Keep Alive = Default is 45000 milliseconds. Enter zero to disable and blank the value to restore the default. ◆ AES Encrypt/Decrypt Key = Displays presence of key, used only if protocol with AES is selected.

Tunnel – Connect Mode Settings (continued)	Description
Reconnect Timer	<p>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.</p> <p>Note:</p> <ul style="list-style-type: none"> ◆ When you configure Tunnel - Connect Mode, you can specify a number of milliseconds to attempt to reconnect after a dropped connection has occurred. The default is 1500 milliseconds. ◆ The Reconnect Timer only applies if a Disconnect Mode is configured. With a Disconnect Mode set, the device server maintains a connection until the disconnect mode condition is met (at which time the device server closes the connection). If the tunnel is dropped due to conditions beyond the device server, the device server attempts to re-establish a failed connection when the specified reconnect interval reaches its limit. ◆ Any network-side disconnect is considered an error and a reconnect is attempted without regard to the Connect Mode settings. Simultaneous Connect Mode connections require some Disconnect Mode configurations or the connections will never terminate. See Tunnel – Disconnect Mode on page 62 for more information about the parameters. ◆ If Disconnect Mode is disabled and the network connection is dropped, then the re-establishment of a tunnel connection is governed by the configured Connect Mode settings.
Flush Serial Data	Select whether to flush the serial line when a connection is made. Choices are: <ul style="list-style-type: none"> ◆ Enabled = flush the serial line when a connection is made. ◆ Disabled = do not flush the serial line. (default)
Block Serial	Select Enabled 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.
Block Network	Select Enabled 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.
Email on Connect	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.
Email on Disconnect	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.
CP Output	<p>Identifies a CP or CP Group whose value should change when a connection is established and when it is dropped.</p> <ul style="list-style-type: none"> ◆ 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.

5. Click **Submit**. The host is configured. A second host appears underneath the newly configured host.
6. Repeat these steps to configure additional hosts as necessary. MatchPort b/g Pro 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 b/g Pro, 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 62](#)). 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 b/g Pro shuts down the specific tunnel connection gracefully.

The following settings end a specific tunnel connection:

- ◆ The MatchPort b/g Pro receives the stop character.
- ◆ The timeout period has elapsed and no activity is going in or out of the MatchPort b/g Pro. Both Accept Mode and Connect Mode must be idle for the time frame.

Figure 6-17 Host 1, Host 2, Host 3 Exchanged

Tunnel 1 Tunnel 2		
Statistics	Serial Settings	Packing Mode
Accept Mode	Connect Mode	Disconnect Mode
Modem Emulation		
Tunnel 2 - Connect Mode		
Mode:	<input style="width: 150px; height: 20px; border: 1px solid #ccc; border-radius: 5px; background-color: #f0f0f0;" type="button" value="Disable"/>	
Local Port:	<input style="width: 150px; height: 20px; border: 1px solid #ccc; border-radius: 5px; background-color: #f0f0f0;" type="button" value="Random"/>	
Host 1:	<input style="width: 150px; height: 20px; border: 1px solid #ccc; border-radius: 5px; background-color: #f0f0f0;" type="button" value="None"/>	
Reconnect Timer:	<input style="width: 80px; height: 20px; border: 1px solid #ccc; border-radius: 5px;" type="text" value="15000"/> milliseconds	
Flush Serial Data:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled	
Block Serial:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled	
Block Network:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled	
Email on Connect:	<input style="width: 150px; height: 20px; border: 1px solid #ccc; border-radius: 5px; background-color: #f0f0f0;" type="button" value="None"/>	
Email on Disconnect:	<input style="width: 150px; height: 20px; border: 1px solid #ccc; border-radius: 5px; background-color: #f0f0f0;" type="button" value="None"/>	
CP Output:	<input style="width: 150px; height: 20px; border: 1px solid #ccc; border-radius: 5px; background-color: #f0f0f0;" type="button" value="Group:"/>	

- The MatchPort b/g Pro 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:

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

Note: Tunnels 3 and 4 do not apply for Modbus b/g Pro embedded device server.

Figure 6-18 Tunnel 1 Disconnect Mode

- Enter or modify the following settings:

Table 6-19 Tunnel Disconnect Mode

Tunnel – Disconnect Mode Settings	Description
Stop Character	Enter the stop character in ASCII, hexadecimal, or decimal notation. Select <None> to disable.
Modem Control	Select Enabled to disconnect when the modem control pin is not asserted on the serial line.
Timeout	Enter a time, in milliseconds, for the 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.

- Click **Submit**.
- 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 b/g Pro, an "OK" message is sent (but the command is silently ignored).

The MatchPort b/g Pro 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

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

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

For ATDT and ATDP commands less than 255 characters, the MatchPort b/g Pro 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 b/g Pro 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.

Figure 6-21 Tunnel 1 Modem Emulation

Configuration		Status
Echo Pluses:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled	
Echo Commands:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	Enabled
Verbose Response:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	Enabled
Response Type:	<input checked="" type="radio"/> Text <input type="radio"/> Numeric	Text
Error Unknown Commands:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled	Disabled
Incoming Connection:	<input checked="" type="radio"/> Disabled <input type="radio"/> Automatic <input type="radio"/> Manual	Disabled
Connect String:	<input type="text"/>	
Display Remote IP:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled	

4. Enter or modify the following settings:

Table 6-22 Tunnel Modem Emulation

Tunnel- Modem Emulation Settings	Description
Echo Pluses	Select Enabled to echo +++ when entering modem Command Mode.
Echo Commands	Select Enabled to echo the modem commands to the console.
Verbose Response	Select Enabled to send modem response codes out on the serial line.
Response Type	Select the type of response code: Text or Numeric .
Error Unknown Commands	Select whether an ERROR or OK response is sent in reply to unrecognized AT commands. Choices are: <ul style="list-style-type: none"> ◆ 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® b/g Pro 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.

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 7-1 Terminal on Line Configuration

Terminal on Line 1 - Configuration	
Terminal Type:	UNKNOWN
Login Connect Menu:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Exit Connect Menu:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Send Break:	<None>
Break Duration:	500 milliseconds
Echo:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled

3. Enter or modify the following settings:

Table 7-2 Terminal on Line 1 Configuration

Terminal on Line Configuration Settings	Description
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.

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.

Figure 7-3 Terminal on Network Configuration

Terminal on Network - Configuration	
Terminal Type:	UNKNOWN
Login Connect Menu:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Exit Connect Menu:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Echo:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled

3. Enter or modify the following settings:

Table 7-4 Terminal on Network Configuration

Terminal on Network Configuration Settings	Description
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.

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.

Figure 7-5 Host Configuration

Host 1	Host 2	Host 3	Host 4
Configuration			
Host 1 - Configuration			
Name:	<input type="text"/>		
Protocol:	<input checked="" type="radio"/> Telnet <input type="radio"/> SSH		
Remote Address:	<input type="text"/>		
Remote Port:	<input type="text" value="0"/>		

- Enter or modify the following settings:

Table 7-6 Host Configuration

Host Settings	Description
Name	Enter a name for the host. This name appears on the Login Connect Menu. To leave a host out of the menu, leave this field blank.
Protocol	Select the protocol to use to connect to the host. Choices are: ◆ Telnet ◆ SSH <i>Note: SSH keys must be loaded or created on the SSH page for the SSH protocol to work.</i>
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.

- Click **Submit** to save changes.
- 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® b/g Pro embedded device server. There are seven configurable pins on the MatchPort b/g Pro.

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 b/g Pro 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 b/g Pro 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 b/g Pro 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 74](#).

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

The screenshot shows the CPM: CPs web page with two main sections: "Current Configuration" and "CP Status".

Current Configuration:

CP	Ref	Configured As	Value	Groups	Active In Group
CP1	P1.13	Input	0	0	<available>
CP2	P1.15	Input	1	0	<available>
CP3	P1.17	Output	0	1	Line1_RS485_Select
CP4	P1.19	Output	0	1	Line1_RS485_HDpx
CP5	P1.29	Input	0	0	<available>
CP6	P1.31	Output	0	1	<available>
CP7	P1.33	Output	0	2	output

CP Status:

Name	CP1								
State	Enabled								
Type	Input	<input type="checkbox"/> Assert Low	<input type="button" value="Change"/>						
Value	0 (0x0)								
Bit	6	5	4	3	2	1	0	-	
Level									
I/O									
Logic									
Binary	x	x	x	x	x	x	0		
CP#								1	
Groups									

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

Table 8-2 CPM CPs Current Configuration

CPM – CPs Current Configuration	Description
CP	Indicates the configurable pin number.
Ref	Indicates the hardware pin number associated with the CP.
Configured As	Shows the CP configuration. A CP configured as Input is set to read input. A CP configured as Output drives data out of the device.
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

CPM – CPs Status	Description
Name	Shows the CP number.
State	Shows the current enable state of the CP.
Type	Indicates whether the CP is set for input or output.
Value	Shows the last bit in the CP current value.
Bit	Visual display of the 32 bit placeholders for a CP.
Level	A “+” symbol indicates the CP is asserted (the voltage is high). A “-“ indicates the CP voltage is low.
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

The screenshot shows the 'CPM: Groups' interface. At the top, there are two tabs: 'CPs' and 'Groups', with 'Groups' being the active tab. Below the tabs, the title 'CPM: Groups' is displayed, followed by 'Current Configuration'. A table lists various groups with their names, states, and assigned CP counts. The table has three columns: 'Group Name', 'State', and 'CP Info'. The 'Group Name' column contains entries like '1', 'I2C', 'Line1_Modem_Ctl_In', etc. The 'State' column indicates if a group is 'Enabled' or 'Disabled'. The 'CP Info' column shows the count of assigned CPs for each group. At the bottom of the interface, there is a 'Create Group:' input field and a 'Group Status' section with a note: 'Click on a Group Name above to view or change.'

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

Create Group:

Group Status

Click on a Group Name above to view or change.

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

Table 8-5 CPM Groups Current Configuration

CPM – Groups Current Configuration	Description
Group (Name)	Shows the CP group's name.
State	Indicates whether the group is enabled or disabled.
CP Info	Indicates the number of CPs assigned to this particular group.

Figure 8-6 CPM: Group Status

To display the status of a specific group:

- Select **CPM > Groups**.
- Select the CP group name in the Current Configuration table.

The screenshot displays the CPM: Groups interface. At the top, there are two tabs: "CPs" and "Groups". The "Groups" tab is selected, showing the "Current Configuration" table below it. The "Group Name" column lists various pins: 1, I2C, Line1_Modem_Ctl_In, Line1_Modem_Ctl_O, Line1_RS485_HDpx, Line1_RS485_Select, Line2_Modem_Ctl_In, Line2_Modem_Ctl_O, Modbus_Ctl_In, Modbus_Ctl_Out, and output. The "State" column indicates the status of each pin, and the "CP Info" column shows the number of CPs assigned. Below the table is a "Create Group:" input field. The main area is titled "Group Status" and shows detailed configuration for the "Line1_Modem_Ctl_O" group. It includes fields for Name (Line1_Modem_Ctl_O), State (Disabled AND Locked, with an "Enable" button), Value (Disabled), Bit (values 6, 5, 4, 3, 2, 1, 0), Level, I/O, Logic, Binary (values X, X, X, X, X, X, X), and CP# (empty). At the bottom, there are buttons for "Add", "CP1" (dropdown), "at bit 0" (dropdown), "as" (dropdown), and "Assert Low" (checkbox).

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

Name	Line1_Modem_Ctl_O							
State	Disabled AND Locked, user may Enable/Disable or Add/Remove CP <input type="button" value="Enable"/>							
Value	Disabled							
Bit	6	5	4	3	2	1	0	
Level								
I/O								
Logic								
Binary	X	X	X	X	X	X	X	
CP#								

Add at bit 0 as Assert Low

Table 8-7 Group Status

CPM – Groups Page Group Status	Description
Name	Shows the CP Group name.
State	Shows the current state of the CP group. Locked groups are Lantronix default groups and cannot be deleted. Use the button in this field to enable or disable the group.
Value	Shows the CP group's current value.
Bit	Displays the individual bit positions for the available CPs.
Level	Indicates the voltage level of the CP. A plus sign (+) indicates the CP bit is asserted (the voltage is high). A minus sign (-) indicates the CP voltage is low.
I/O	Indicates the current status of the pin: ◆ I = input ◆ O = output ◆ <blank> = unassigned
Logic	Indicates the 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 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.

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® b/g Pro embedded device server 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

The screenshot shows the 'DNS' configuration page. At the top, there's a 'Current Status' section with three rows: 'Domain' (eng.lantronix.com), 'Primary DNS' (172.19.1.1 (DHCP)), and 'Secondary DNS' (172.19.1.2 (DHCP)). Below this is a search bar with a 'Lookup' button. The bottom section is titled 'Cache Entries' and displays the message 'There are no entries in the cache.' with a '[Remove All]' link.

Current Status	
Domain:	eng.lantronix.com
Primary DNS:	172.19.1.1 (DHCP)
Secondary DNS:	172.19.1.2 (DHCP)

[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 b/g Pro 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 b/g Pro 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 b/g Pro also supports authentication scheme of “None” when no authentication is required during link negotiation.

Since the MatchPort b/g Pro 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 b/g Pro Web Manager or CLI to configure a network link using PPP over a serial line. Turn off Connect Mode, Accept Mode, and Command mode before enabling PPP. The MatchPort 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 b/g Pro does not perform network address translation (NAT) between the serial-side network interface and the Ethernet/WLAN network interface. Therefore, to pass packets through the MatchPort, 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 b/g Pro 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 b/g Pro 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 b/g Pro).

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.

Figure 9-2 PPP Configuration Settings

Line 1 Line 2

Configuration

PPP on Line 1 - Configuration

WARNING: Serial protocol is not PPP.

Local IP Address:	<None>
Peer IP Address:	<None>
Authentication Mode:	<input type="radio"/> None <input checked="" type="radio"/> PAP <input type="radio"/> CHAP <input type="radio"/> MS-CHAP <input type="radio"/> MS-CHAPV2
Username:	
Password:	<None>

Submit

3. Enter or modify the following settings:

Table 9-3 PPP Configuration

PPP Configuration Settings	Description
Local IP Address	Enter the IP address assigned to the device's PPP interface.
Peer IP Address	Enter the IP address assigned to the peer (when requested during negotiation).
Authentication Mode	Choose the authentication mode: <ul style="list-style-type: none"> ◆ None = no authentication is required ◆ PAP = Password Authentication Protocol ◆ CHAP = Challenge Handshake Authentication Protocol ◆ MS-CHAP = Microsoft Challenge-Handshake Authentication Protocol ◆ MS-CHAPV2 = Microsoft Challenge-Handshake Authentication Protocol Version 2

PPP Configuration Settings	Description
Username	Enter a username if authentication is to be used on the PPP interface. The peer must be configured to use the same username.
Password	Enter a password if authentication is to be used on the PPP interface. The peer must be configured to use the same password.

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

SNMP	
State:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Read Community:	<Configured>
Write Community:	<Configured>
System Contact:	
System Name:	xport_pro
System Description:	<input type="text"/> <Default> Lantronix XPort Pro V5.2.0.0R12 (07092877T7DGFL)
System Location:	
Traps State:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Traps Primary Destination:	
Traps Secondary Destination:	

Note: The system description string will reflect the specific Lantronix product.

2. Enter or modify the following settings:

Table 9-5 SNMP

SNMP Settings	Description
State	Select Enabled to enable SNMP.

SNMP Settings (continued)	Description
Read Community	Enter the SNMP read-only community string.
Write Community	Enter the SNMP read/write community string.
System Contact	Enter the name of the system contact.
System Name	Enter the system name.
System Description	Enter the system description.
System Location	Enter the system location.
Traps State	Select Enabled 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.
Traps Primary Destination	Enter the primary SNMP trap host.
Traps Secondary Destination	Enter the secondary SNMP trap host.

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

Configuration	
State:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Admin Username:	admin
Admin Password:	<Configured>

Statistics	
Status:	Running
Connections Rejected:	0
Connections Accepted:	0
Active Connections:	0
Last Client:	No device has connected

2. Enter or modify the following settings:

Table 9-7 FTP Settings

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

3. Click **Submit**.

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:

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

Figure 9-8 TFTP Configuration

TFTP Server	
Configuration	
State:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Allow File Creation:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Allow Firmware Update:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Allow XCR Import:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Statistics	
Status:	Running
Files Downloaded:	0
Files Uploaded:	0
File Not Found Errors:	0
File Read Errors:	0
File Write Errors:	0
Unknown Errors:	0
Last Client:	No device has connected

- Enter or modify the following settings:

Table 9-9 TFTP Server

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

- 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

Configuration	
State:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Host:	172.19.39.23
Local Port:	514
Remote Port:	514
Severity Log Level:	Debug

Statistics	
Status:	Running
Messages Sent:	484
Messages Failed:	0

2. Enter or modify the following settings:

Table 9-11 Syslog

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

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 b/g Pro 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

The screenshot shows a web-based interface for viewing HTTP statistics. At the top, there are three tabs: 'Statistics' (which is selected and highlighted in grey), 'Configuration', and 'Authentication'. Below the tabs, the title 'HTTP Statistics' is centered. A table follows, displaying various metrics and their values. The table has two columns: the left column lists the metric names, and the right column lists their corresponding values. At the bottom of the table, there is a note about logs.

Rx Bytes	26295
Tx Bytes	198244
200 - OK	15
301 - Moved Permanently	0
400 - Bad Request	0
401 - Authorization Required	13
404 - Not Found	0
408 - Request Timeout	0
413 - Request Too Large	0
500 - Internal Error	0
501 - Not Implemented	0
Status Unknown	0
Work Queue Full	0
Socket Error	0
Memory Error	0
Logs:	42 entries (6291 bytes) [View] [Clear]

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

The screenshot shows the 'HTTP Configuration' page with the following settings:

HTTP Configuration	
State:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Port:	80
Secure Port:	443
Secure Protocols:	<input checked="" type="checkbox"/> SSL3 <input checked="" type="checkbox"/> TLS1.0 <input checked="" type="checkbox"/> TLS1.1
Max Timeout:	10 seconds
Max Bytes:	40960
Logging State:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Max Log Entries:	50
Log Format:	%h %t "%r" %s %B "%{Referer}i" "%{User-Agent}i"
Authentication Timeout:	30 minutes

2. Enter or modify the following settings:

Table 9-14 HTTP Configuration

HTTP Configuration Settings	Description
State	Select Enabled to enable the HTTP server.
Port	Enter the port for the HTTP server to use. The default is 80 .
Secure Port	Enter the port for the HTTPS server to use. The default is 443 . The HTTP server only listens on the HTTPS Port when an SSL certificate is configured.

HTTP Configuration Settings (continued)	Description
Secure Protocols	Select to enable or disable the following protocols: <ul style="list-style-type: none"> ◆ SSL3 = Secure Sockets Layer version 3 ◆ TLS1.0 = Transport Layer Security version 1.0. TLS 1.0 is the successor of SSL3 as defined by the IETF. ◆ TLS1.1 = Transport Layer Security version 1.1 The protocols are enabled by default. Note: A server certificate and associated private key need to be installed in the SSL configuration section to use HTTPS .
Max Timeout	Enter the maximum time for the HTTP server to wait when receiving a request. This prevents Denial-of-Service (DoS) attacks. The default is 10 seconds.
Max Bytes	Enter the maximum number of bytes the HTTP server accepts when receiving a request. The default is 40 KB (this prevents DoS attacks).
Logging State	Select Enabled to enable HTTP server logging.
Max Log Entries	Sets the maximum number of HTTP server log entries. Only the last Max Log Entries are cached and viewable.
Log Format	Set the log format string for the HTTP server. Follow these Log Format rules: <ul style="list-style-type: none"> ◆ %a - remote IP address (could be a proxy) ◆ %b - bytes sent excluding headers ◆ %B - bytes sent excluding headers (0 = '-') ◆ %h - remote host (same as '%a') ◆ %{h}i - header contents from request (h = header string) ◆ %m - request method ◆ %p - ephemeral local port value used for request ◆ %q - query string (prepend with '?' or empty '-') ◆ %t - timestamp HH:MM:SS (same as Apache '%(%H:%M:%S)t' or '%(%T)t') ◆ %u - remote user (could be bogus for 401 status) ◆ %U - URL path info ◆ %r - first line of request (same as '%m %U%q <version>') ◆ %s - return status
Authentication Timeout	The timeout period applies if the selected authentication type is either Digest or SSL/Digest . After this period of inactivity, the client must authenticate again.

3. Click **Submit**.

HTTP Authentication

HTTP Authentication enables you to require usernames and passwords to access specific web pages or directories on the MatchPort b/g Pro' 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.

Figure 9-15 HTTP Authentication

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

2. Enter or modify the following settings:

Table 9-16 HTTP Authentication

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

HTTP Authentication Settings (continued)	Description
Auth Type	<p>Select the authentication type:</p> <ul style="list-style-type: none"> ◆ 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. <p>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.</p>
Username	<p>Enter the Username used to access the URI. More than one Username per URI is permitted.</p> <p>Click Submit and enter the next Username as necessary.</p>
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 b/g Pro 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 b/g Pro configuration changes, RSS feeds permit viewing only relevant and new information regarding changes made to the MatchPort b/g Pro 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

Configuration	
RSS Feed:	<input type="radio"/> On <input checked="" type="radio"/> Off
Persistent:	<input type="radio"/> On <input checked="" type="radio"/> Off
Max Entries:	100

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

2. Enter or modify the following settings:

Table 9-18 RSS

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

3. Select **Submit**.
4. In the **Current Status** table, view and clear stored RSS Feed entries, as necessary.

LPD Settings

The MatchPort b/g Pro 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

The screenshot shows a web-based interface for LPD statistics. At the top, there are two tabs: "LPD 1" (which is active) and "LPD 2". Below the tabs is a horizontal menu bar with three items: "Statistics" (which is active), "Configuration", and "Print Test Page". The main content area is titled "LPD 1 - Statistics". It contains a table with four rows:

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

Banner:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Binary:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Start of Job:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
End of Job:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Formfeed:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Convert Newlines:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
SOJ String:	<input type="text"/> <input checked="" type="radio"/> Text <input type="radio"/> Binary
EOJ String:	<input type="text"/> <input checked="" type="radio"/> Text <input type="radio"/> Binary
Queue Name:	<input type="text"/>

2. Enter or modify the following settings:

Table 9-21 LPD Configuration

LPD Configuration Settings	Description
Banner	Select Enabled to print the banner even if the print job does not specify to do so. Selected by default.
Binary	Select Enabled for the 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.
Start of Job	Select Enabled to print a "start of job" string before sending the print data.
End of Job	Select Enabled to send an "end of job" string.

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

- Click **Submit**. Repeat above steps as desired, according to additional LPD lines available on your product.

10: Security Settings

The MatchPort® b/g Pro 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 b/g Pro supports SSLv3 and its successors, TLS1.0 and TLS1.1. An incoming SSIV2 connection attempt is answered with an SSIV3 response. If the initiator also supports SSIV3, SSIV3 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 15: Security in Detail on page 155](#).*

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 b/g Pro 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 b/g Pro 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 b/g Pro 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 EDS.

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.

Figure 10-1 SSH Server: Host Keys (Upload Keys)

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

5. Enter or modify the following settings in the part of the screen related to uploading keys:

Table 10-2 SSH Server Host Keys Settings - Upload Keys Method

SSH Server: Host Keys Settings (continued)	Description
Private Key	Enter the path and name of the existing private key you want to upload or use the Browse button to select the key. Be sure the private key will not be compromised in transit. This implies the data is uploaded over some kind of secure private network.
Public Key	Enter the path and name of the existing public key you want to upload or use the Browse button to select the key.
Key Type	Select a key type to use for the new key: <ul style="list-style-type: none"> ◆ 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.

```
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 \(on page 99\)](#).

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.

Figure 10-3 SSH Server: Host Keys (Upload Keys)

The screenshot shows the 'SSH Server: Host Keys' configuration page. At the top, there are two tabs: 'SSH Server: Host Keys' (selected) and 'SSH Client: Known Hosts'. Below them are two more tabs: 'SSH Server: Authorized Users' and 'SSH Client: Users'. The main section is titled 'SSH Server: Host Keys' and contains two sub-sections: 'Upload Keys' and 'Create New Keys'. In the 'Upload Keys' section, there are fields for 'Private Key' and 'Public Key', each with a 'Browse...' button. Below these is a 'Key Type' selection with radio buttons for 'RSA' and 'DSA', and a 'Submit' button. In the 'Create New Keys' section, there are similar fields for 'Key Type' (radio buttons for RSA and DSA) and 'Bit Size' (radio buttons for 512, 768, and 1024), followed by a 'Submit' button. A horizontal line separates this from the 'Current Configuration' section, which displays two tables: one for 'Public RSA Key' (No RSA Key Configured) and one for 'Public DSA Key' (No DSA Key Configured).

SSH Server: Host Keys Settings (continued)		Description
Private Key	Enter the path and name of the existing private key you want to upload or use the Browse button to select the key. Be sure the private key will not be compromised in transit. This implies the data is uploaded over some kind of secure private network.	
Public Key	Enter the path and name of the existing public key you want to upload or use the Browse button to select the key.	
Key Type	Select a key type to use for the new key: <ul style="list-style-type: none"> ◆ RSA = use this key with the SSH1 and SSH2 protocols. ◆ DSA = use this key with the SSH2 protocol. 	

- 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

SSH Server: Host Keys Settings (continued)		Description
Private Key	Enter the path and name of the existing private key you want to upload or use the Browse button to select the key. Be sure the private key will not be compromised in transit. This implies the data is uploaded over some kind of secure private network.	
Public Key	Enter the path and name of the existing public key you want to upload or use the Browse button to select the key.	
Key Type	Select a key type to use for the new key: <ul style="list-style-type: none"> ◆ RSA = use this key with the SSH1 and SSH2 protocols. ◆ DSA = use this key with the SSH2 protocol. 	

- Click **Submit**.

Note: SSH keys may be created on another computer and uploaded to the MatchPort b/g Pro. 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.

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

The screenshot shows the 'SSH Server: Host Keys' configuration page. At the top, there are four tabs: 'SSH Server: Host Keys' (selected), 'SSH Client: Known Hosts', 'SSH Server: Authorized Users', and 'SSH Client: Users'. Below the tabs, the main section is titled 'SSH Server: Host Keys'. It contains two main sections: 'Upload Keys' and 'Create New Keys'. Under 'Upload Keys', there are fields for 'Private Key' and 'Public Key' with 'Browse...' buttons, and radio buttons for 'Key Type' (RSA or DSA). A 'Submit' button is below these fields. Under 'Create New Keys', there are radio buttons for 'Key Type' (RSA or DSA) and 'Bit Size' (512, 768, or 1024), followed by another 'Submit' button. At the bottom, the 'Current Configuration' section displays two tables: one for 'Public RSA Key' (No RSA Key Configured) and one for 'Public DSA Key' (No DSA Key Configured).

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

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

SSH Server: Host Keys Settings	Description
Key Type	<p>Select a key type to use:</p> <ul style="list-style-type: none"> ◆ RSA = use this key with SSH1 and SSH2 protocols. ◆ DSA = use this key with the SSH2 protocol. <p>Note: RSA is more secure.</p>

SSH Server: Host Keys Settings (continued)		Description
Bit Size	<p>Select a bit length for the new key:</p> <ul style="list-style-type: none"> ◆ 512 ◆ 768 ◆ 1024 <p>Using a larger bit size takes more time to generate the key. Approximate times are:</p> <ul style="list-style-type: none"> ◆ 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 <p>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.</p>	

3. Click **Submit**.

Note: SSH Keys from other programs may be converted to the required MatchPort b/g Pro 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 b/g Pro 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.

Figure 10-7 SSH Server: Authorized Users

SSH Server: Authorized Users

Username:

Password:

Public RSA Key:

Public DSA Key:

Current Configuration

User:	guest [Delete User]
Password:	Configured
Public RSA Key:	No RSA Key Configured
Public DSA Key:	No DSA Key Configured

2. Enter or modify the following settings:

Table 10-8 SSH Server Authorized User Settings

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

3. Click **Submit**.

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.

Figure 10-9 SSH Client: Known Hosts

2. Enter or modify the following settings:

Table 10-10 SSH Client Known Hosts

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

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 b/g Pro 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

The screenshot shows the 'SSH Client: Users' configuration page. At the top, there are four tabs: 'SSH Server: Host Keys', 'SSH Client: Known Hosts', 'SSH Server: Authorized Users', and 'SSH Client: Users'. The 'SSH Client: Users' tab is highlighted. Below the tabs, there is a form with the following fields:

- Username:** Text input field.
- Password:** Text input field.
- Remote Command:** Text input field.
- Private Key:** Text input field with a **Browse...** button.
- Public Key:** Text input field with a **Browse...** button.
- Key Type:** Radio buttons for **RSA** and **DSA**.
- Add/Edit**: A blue button.

Below the form is a section titled **Create New Keys** with the following fields:

- Username:** Text input field.
- Key Type:** Radio buttons for **RSA** and **DSA**.
- Bit Size:** Radio buttons for **512**, **768**, and **1024**.
- Submit**: A blue button.

At the bottom of the page is a section titled **Current Configuration** with the message: **No Users are currently configured for the SSH Client.**

2. Enter or modify the following settings:

Table 10-12 SSH Client Users

SSH Client: Users Settings	Description
Username	Enter the name that the device uses to connect to a SSH server.
Password	Enter the password associated with the username.
Remote Command	Enter the command that can be executed remotely. Default is shell , which tells the SSH server to execute a remote shell upon connection. This command can be changed to anything the remote host can perform.
Private Key	Enter the name of the existing private key you want to use with this SSH client user. You can either enter the path and name of the key, or use the Browse button to select the key.
Public Key	Enter the path and name of the existing public key you want to use with this SSH client user or use the Browse button to select the key. 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
Key Type	Select the key type to be used. Choices are: <ul style="list-style-type: none"> ◆ RSA = use this key with the SSH1 and SSH2 protocols. ◆ DSA = use this key with the SSH2 protocol.
Create New Keys	
Username	Enter the name of the user associated with the new key.
Key Type	Select the key type to be used for the new key. Choices are: <ul style="list-style-type: none"> ◆ RSA = use this key with the SSH1 and SSH2 protocols. ◆ DSA = use this key with the SSH2 protocol.
Bit Size	Select the bit length of the new key: <ul style="list-style-type: none"> ◆ 512 ◆ 768 ◆ 1024 Using a larger Bit Size takes more time to generate the key. Approximate times are: <ul style="list-style-type: none"> ◆ 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 \(on page 106\)](#).

SSL uses digital certificates for authentication and cryptography against eavesdropping and tampering. Sometimes only the server is authenticated, sometimes both server and client. The MatchPort b/g Pro 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 b/g Pro supports SSIV3 and its successors, TLS1.0 and TLS1.1.

Note: An incoming SSIV2 connection attempt is answered with an SSIV3 response. If the initiator also supports SSIV3, SSIV3 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 10-13 Supported Cipher Suites

Certificate	Key Exchange	Encryption	Hash
DSA	DHE	3DES	SHA1
RSA	RSA	128 bits AES	SHA1
RSA	RSA	Triple DES	SHA1
RSA	RSA	128 bits RC4	MD5
RSA	RSA	128 bits RC4	SHA1
RSA	1024 bits RSA	56 bits RC4	MD5
RSA	1024 bits RSA	56 bits RC4	SHA1
RSA	1024 bits RSA	40 bits RC4	MD5

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

SSL Certificates

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

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

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

An authority that signs 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, SSL Tunneling in Accept mode, and/or EAP-TLS, the MatchPort b/g Pro needs a personal certificate with a matching private key to identify itself and sign its messages. When using SSL Tunneling in Connect mode and/or EAP-TLS, EAP-TTLS or PEAP, the MatchPort b/g Pro 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 b/g Pro 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 b/g Pro, only those key exchange methods that can work with that style certificate are enabled. RSA is sufficient in most cases.

SSL Certificates and Private Keys

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

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

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

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

Steel Belted RADIUS

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

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

The sbr_certkey.pem file contains both certificate and key. If loading the SBR certificate into MatchPort b/g Pro as an authority, you will need to edit it.

1. Open the file in any plain text editor.
2. Delete all info before the following: "----- BEGIN CERTIFICATE-----"
3. Delete all info after the following: "----- END CERTIFICATE-----"
4. Save as sbr_cert.pem. SBR accepts trusted-root certificates in the DER format.
5. Again, OpenSSL can convert any format into DER by using the following commands in the order shown:

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

Note: With SBR, when the identity information includes special characters such as dashes and periods, SBR changes the format it uses to store these strings and becomes incompatible with the current MatchPort b/g Pro release. We will add support for this and other formats in future releases. Free RADIUS—Linux open-source RADIUS server. It is versatile, but complicated to configure.

Free RADIUS

Free RADIUS is a Linux open-source RADIUS server. It is versatile, but complicated to configure.

SSL Configuration

To configure SSL settings:

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

Figure 10-14 SSL

The screenshot shows the SSL configuration interface. It includes sections for uploading a certificate and authority, creating a self-signed certificate, and displaying current certificates and authorities.

Upload Certificate

- New Certificate:
- New Private Key:
-

Upload Authority Certificate

- Authority:
-

Create New Self-Signed Certificate

- Country (2 Letter Code):
- State/Province:
- Locality (City):
- Organization:
- Organization Unit:
- Common Name:
- Expires: mm/dd/yyyy
- Key length: 512 bit 768 bit 1024 bit
- Type: RSA DSA
-

Current SSL Certificates
<None>

Current Certificate Authorities
<None>

2. Enter or modify the following settings:

Table 10-15 SSL

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

SSL Settings (continued)	Description
Common Name	Enter the same name that the user will enter when requesting your web site. Example: If a user enters http://www.widgets.abccompany.com to access your web site, the Common Name would be www.widgets.abccompany.com .
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: <ul style="list-style-type: none"> ◆ 512 bits ◆ 768 bits ◆ 1024 bits The larger the bit size, the longer it takes to generate the key. Approximate times are: <ul style="list-style-type: none"> ◆ 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: <ul style="list-style-type: none"> ◆ 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

Transaction ID (2 bytes)	Identification of request/response transaction - copied by slave
Protocol ID (2 bytes)	0 - Modbus protocol
Length (2 bytes)	Number of following bytes includes the unit identifier
Address (1 byte)	Identification of remote slave

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 74 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® b/g Pro embedded device server. The Modbus 'local slave' supported functions are listed in the table below.

Table 11-2 Modbus Local Slave Functions - Query

Name	Number	Address Hi [0]	Address Lo [1]	Data Hi [2]	Data Lo [3]	Bytes Count [4]	Value [5]
Read Coils	0x01	0x00	0x00-0x02 Starting CP CP1 – CP3	0x00	0x01-0x03 No of CPs to output	N/A	N/A
Read Input status	0x02	0x00	0x00-0x02 Starting CP CP1 – CP3	0x00	0x01-0x03 No of CPs to output	N/A	N/A
Read Holding Registers	0x03	0x00	0x00-0x02 Starting CP CP1 – CP3	0x00	0x01-0x03 No of CPs to output	N/A	N/A
Read Input Registers	0x04	0x00	0x00-0x02 Starting CP CP1 – CP3	0x00	0x01-0x03 No of CPs to output	N/A	N/A

Name	Number	Address Hi [0]	Address Lo [1]	Data Hi [2]	Data Lo [3]	Bytes Count [4]	Value [5]
Force Single Coil	0x05	0x00	0x00-0x02 Output CP CP1 – CP3	0xff (set CPx to 1) or 0x00 (set CPx to 0)	0x00	N/A	N/A
Preset Single Register	0x06	0x00	0x00-0x02 CP1 – CP3	0x00	0x00 or 0x01	N/A	N/A
Force Multiple Coils	0x0F	0x00	0x00-0x02 Starting CP CP1 – CP3	0x00	0x01-0x03 No of CPs to set	0x01	0B00000xyz CP values ,Lo CP# in low bit
Preset Multiple Registers	0x10	0x00	0x00-0x02 Starting CP CP1 – CP3	0x00	0x01-0x03 No of CPs to set	0x02-0x06 (No of CPs to set) * 2	Max [6].. 0x00, 0x0Y 0x00 ,0x0Y 0x00, 0x0Y Y = 0 or 1
Read/Write 4X Registers	0x17	0x00	0x00-0x02 Starting CP CP1 – CP3 to read	0x00	0x01-0x03 Quantity to read	0x00	0x00-0x02 Starting CP CP1 – CP3 to write
		0x00	0x01-0x03 Quantity to write	0x02-0x06 (Quantity to write) * 2	Max [6].. 0x00, 0x0Y 0x00 ,0x0Y 0x00, 0x0Y Y = 0 or 1		

Table 11-3 Modbus Local Slave Functions - Response

Name	Number	Byte Count	Data [0]	Data [1]	Data [2]	Data [3]	Data [4]	Data [5]
Read Coils	0x01	0x01	0B00000xyz CP output values ,Lo CP# in high bit	N/A	N/A	N/A	N/A	N/A
Read Input status	0x02	0x01	0B00000xyz CP output values ,Lo CP# in high bit	N/A	N/A	N/A	N/A	N/A
Read Holding Registers	0x03	0x02-0x06	0x00	Starting CP Value 0x00 or 0x01	0x00	Next CP or End CP value 0x00 or 0x01	0x00	End CP value 0x00 or 0x01
Read Input Registers	0x04	0x02-0x06	0x00	Starting CP Value 0x00 or 0x01	0x00	Next CP or End CP value 0x00 or 0x01	0x00	End CP value 0x00 or 0x01
Force Single Cell	0x05	Echo query	Echo query	Echo query	Echo query	N/A	N/A	N/A
Preset Single Register	0x06	Echo query	Echo query	Echo query	Echo query	N/A	N/A	N/A

Name	Number	Byte Count	Data [0]	Data [1]	Data [2]	Data [3]	Data [4]	Data [5]
Force Multiple Coil	0x0F	Echo query	Echo query	Echo query	Echo query	N/A	N/A	N/A
Preset Multiple Registers	0x10	Echo query	Echo query	Echo query	Echo query	N/A	N/A	N/A
Read/ Write 4X Registers	0x17	0x02-0x06 (Quantity of Read) * 2	Max [6]. 0x00, 0x0Y 0x00 ,0x0Y 0x00, 0x0Y Y = 0 or 1					

Serial Transmission Mode

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

RTU	ASCII
<ul style="list-style-type: none"> ◆ Address: 8 bits (0 to 247 decimal, 0 is used for broadcast) ◆ Function: 8 bits (1 to 255, 0 is not valid) ◆ Data: N X 8 bits (N=0 to 252 bytes) ◆ CRC Check: 16 bits 	<ul style="list-style-type: none"> ◆ Address: 2 CHARS ◆ Function: 2 CHARS ◆ Data: N CHARS (N=0 to 252 CHARS) ◆ LRC Check: 2 CHARS

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

The screenshot shows a web-based monitoring interface for Modbus statistics. At the top, there are two tabs: "Statistics" (which is selected) and "Configuration". Below the tabs, the title "Modbus Statistics" is centered. The main content is organized into three sections: "TCP Server", "Additional TCP Server", and "Local Slave".

TCP Server	
State:	Up
Port:	502
Last Connection:	local:502 <- 172.19.205.10:3903
Uptime:	0 days 02:38:20
Total PDUs In:	0
Total PDUs Out:	0
Total Connections:	1
Current Connections:	local:502 <- 172.19.205.10:3903 [Kill] Uptime: 0 days 02:36:48 PDUs In: 0 PDUs Out: 0

Additional TCP Server	
State:	Up
Port:	505
Last Connection:	<None>
Uptime:	0 days 02:35:53
Total PDUs In:	0
Total PDUs Out:	0
Total Connections:	0
Current Connections:	<None>

Local Slave	
Total PDUs In:	0
Total PDUs Out:	0
Exception Count:	0

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.

Figure 11-6 Modbus Configuration

The screenshot shows a web-based configuration interface for a Modbus server. At the top, there are two tabs: "Statistics" and "Configuration". The "Configuration" tab is selected. Below the tabs, the title "Modbus Configuration" is displayed. The configuration area contains four rows of settings:

TCP Server State:	<input type="radio"/> On <input checked="" type="radio"/> Off
Additional TCP Server Port:	<None>
Response Timeout:	3000 milliseconds
RSS Trace Input:	<input type="radio"/> On <input checked="" type="radio"/> Off

2. Enter or modify the following settings:

Table 11-7 Modbus Configuration

Modbus Configuration Settings	Description
TCP Server State	If On , the Modbus server is active on TCP 502.
Additional TCP Server Port	If present, is used in addition to TCP port 502.
Response Timeout	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.
RSS Trace Input	If On , each PDU received on the Modbus serial line creates a non-persistent descriptive item in the RSS feed.

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 45](#) 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 MatchPort® b/g Pro 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.

Figure 12-1 Filesystem Statistics

Filesystem Statistics	
Statistics	Browse
Filesystem Size:	7.500000 Mbytes (7864320 bytes)
Available Space:	7.474250 Mbytes (7837320 bytes) (99%)
Clean Space:	7.336588 Mbytes (7692972 bytes) (97%)
Dirty Space:	140.964 Kbytes (144348 bytes) (1%)
File & Dir Space Used:	26.367 Kbytes (27000 bytes) (0%)
Data Space Used:	22.650 Kbytes (23194 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:	08 - 67, 0 erase cycles
Bank B Sectors:	68 - 127, 2 erase cycles
Busy:	No
Actions:	
[Compact] [Format]	

The configuration gets retained.

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.

Figure 12-2 Filesystem Browser

The screenshot shows the 'Filesystem Browser' interface with the following sections:

- Header:** Statistics
- Path:** /
- Create:**
 - File:
 - Directory:
- Upload File:**
 -
 -
- Copy File:**
 - Source:
 - Destination:
 -
- Move:**
 - Source:
 - Destination:
 -
- TFTP:**
 - Action: Get Put
 - Mode: ASCII Binary
 - Local File:
 - Remote File:
 - Host:
 - Port:
 -

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

Filesystem Browser Settings	Description
Create	
File	Enter the name of the file you want to create, and then click Create .
Directory	Enter the name of the directory you want to create, and then click Create .
Upload File	Enter the path and name of the file you want to upload by means of HTTP/HTTPS or use the Browse button to select the file, and then click Upload .
Copy File	
Source	Enter the location where the file you want to copy resides.
Destination	Enter the location where you want the file copied. After you specify a source and destination, click Copy to copy the file.
Move	
Source	Enter the location where the file you want to move resides.
Destination	Enter the location where you want the file moved. After you specify a source and destination, click Move to move the file.
TFTP	
Action	Select the action that is to be performed via TFTP: Get = a “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**.

Figure 12-4 TCP Protocol

3. Modify the following settings:

Table 12-5 TCP Protocol Settings

Protocol Stack TCP Settings	Description
Send RSTs	Click Enabled to send RSTs or Disabled to stop sending RSTs. TCP contains six control bits, with one or more defined in each packet. RST is one of the control bits. The RST bit is responsible for telling the receiving TCP stack to end a connection immediately. Note: Setting the RSTs may pose a security risk.
Ack Limit	Enter a number to limit how many packets get received before an ACK gets forced. If there is a large amount of data to acknowledge, an ACK gets forced. If the sender TCP implementation waits for an ACK before sending more data even though the window is open, setting the Ack Limit to 1 packet improves performance by forcing immediate acknowledgements.
Send Data	The Send Data selection governs when data may be sent into the network. The Standard implementation waits for an ACK before sending a packet less than the maximum length. Select Expedited to send data whenever the window allows it.

Protocol Stack TCP Settings	Description
Max Retrans	Enter the maximum number of retransmissions of a packet that will be attempted before failing.
Max Retrans Syn/Ack	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.
Max Timeout	Enter the maximum time between retransmissions.

4. Click **Submit**.

IP Settings

To configure the network protocol settings for IP:

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

Figure 12-6 IP Protocol

TCP	IP	ICMP	ARP	SMTP
IP				
Configuration				
IP Time to Live:	64	hops		
Multicast Time to Live:	1	hops		

3. Modify the following settings:

Table 12-7 IP Protocol Settings

Protocol Stack IP Settings	Description
IP Time to Live	This value typically fills the Time To Live in the IP header. SNMP refers to this value as "ipDefaultTTL". Enter the number of hops to be transmitted before the packet is discarded.
Multicast Time to Live	This value fills the Time To Live in any multicast IP header. Normally this value will be one so the packet will be blocked at the first router. It is the number of hops allowed before a Multicast packet is discarded. Enter the value to be greater than one to intentionally propagate multicast packets to additional routers.

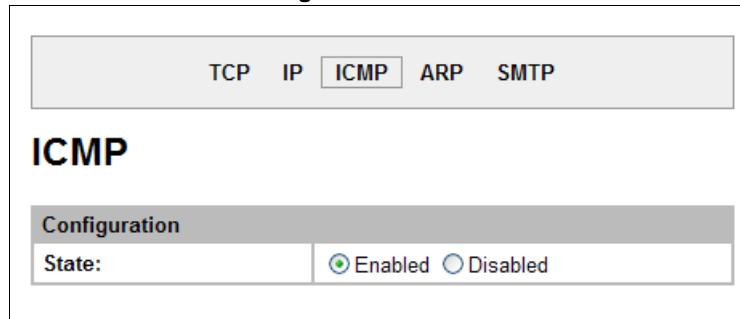
4. Click **Submit**.

ICMP Settings

To configure the ICMP network protocol:

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

Figure 12-8 ICMP Protocol



3. Select the appropriate state.

Table 12-9 ICMP Settings

Protocol Stack ICMP Settings	Description
State	The State selection is used to turn on/off processing of ICMP messages. This includes both incoming and outgoing messages. Choose Enabled or Disabled .

4. Click **Submit**.

ARP Settings

To configure the ARP network protocol:

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

Figure 12-10 ARP Protocol Page

The screenshot shows the ARP Protocol configuration page. At the top, there is a navigation bar with tabs: TCP, IP, ICMP, ARP (which is selected and highlighted in blue), and SMTP. Below the navigation bar, the word "ARP" is displayed in large bold letters. Under "ARP", there is a "Configuration" section containing a table for setting the ARP Timeout. The table has three rows: "0 hours", "1 minutes", and "0 seconds". In the middle of the page, there is a "ARP Cache" section. It includes fields for "IP Address" and "MAC Address", and a "Add" button. Below these fields is a table listing current ARP cache entries. The table has columns: Address, Age Sec, MAC Address, Type, and Interface. The entries are as follows:

Address	Age Sec	MAC Address	Type	Interface
172.19.100.3 [Remove]	8.0	00:16:76:b1:e3:f0	Dynamic	1
172.19.217.2 [Remove]	43.3	00:25:11:8b:c1:f3	Dynamic	1
172.19.39.20 [Remove]	41.8	00:04:23:0e:19:36	Dynamic	1
172.19.1.1 [Remove]	18.4	00:1b:21:0e:3d:f4	Dynamic	1
172.19.0.1 [Remove]	7.7	00:d0:04:02:c0:00	Dynamic	1
172.19.250.250 [Remove]	0.0	00:25:11:3f:47:4d	Dynamic	1
172.19.100.181 [Remove]	15.7	00:15:17:4a:6d:51	Dynamic	1
172.19.39.23 [Remove]	6.2	00:17:31:47:19:71	Dynamic	1

At the bottom of the cache section, there is a "[Remove All]" button.

3. Modify the following settings:

Table 12-11 ARP Settings

Protocol Stack ARP Settings	Description
ARP Timeout	This is the maximum duration an address remains in the cache. Enter the time, in hours , minutes and seconds .
IP Address	Enter the IP address to add to the ARP cache.

Table 12-11 ARP Settings

Protocol Stack ARP Settings (continued)	Description
MAC Address	Enter the MAC address to add to the ARP cache.

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.

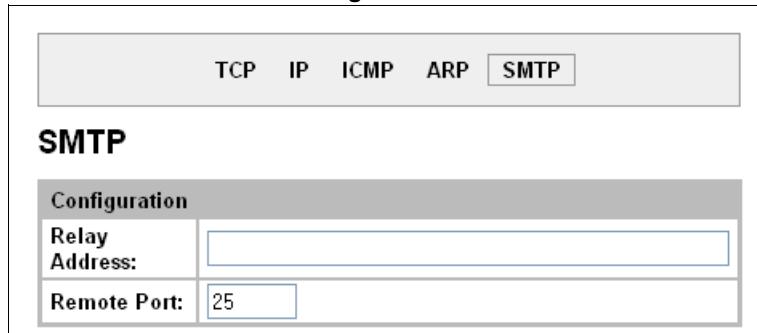
SMTP Settings

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**.

Figure 12-12 SMTP

3. Modify the following settings:

Table 12-13 SMTP Settings

Protocol Stack SMTP Settings	Description
Relay Address	Address of all outbound email messages through a mail server. Can contain either a hostname or an IP address.
Remote Port	Port utilized for the delivery of outbound email messages.

4. Click **Submit**.

IP Address Filter

The IP address filter specifies the hosts and subnets permitted to communicate with the MatchPort b/g Pro device. 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.

Figure 12-14 IP Address Filter Configuration

The figure shows a web-based configuration interface for an IP Address Filter. At the top, it says "IP Address Filter". Below that are two input fields: "IP Address:" and "Network Mask:", each with a corresponding text input box. Underneath these fields is a blue "Add" button. A horizontal line separates this from the "Current State" section. In the "Current State" section, the text "The IP Filter Table is empty so ALL addresses are allowed." is displayed in a grey font.

Note: If you enter any filter, be careful to make sure that your network IP address is covered. Otherwise you will lose access to the MatchPort b/g Pro. You will have to then access the MatchPort from a different computer to reset the configuration.

2. Enter or modify the following settings:

Table 12-15 IP Address Filter Settings

IP Address Filter Settings	Description
IP Address	Enter the IP address to add to the IP filter table.
Network Mask	Enter the IP address' network mask in dotted notation.

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 \(on page 21\)](#).

To configure the query port server:

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

Figure 12-16 Query Port Configuration

The screenshot shows the 'Query Port' configuration page. At the top, there is a section for enabling or disabling the 'Query Port Server'. A radio button labeled 'On' is selected, while 'Off' is unselected. Below this is a 'Submit' button. The main area is titled 'Current Configuration and Statistics' and contains a table with the following data:

Query Port Status:	On (running)
In Valid Queries:	135
In Unknown Queries:	124
In Erroneous Packets:	0
Out Query Replies:	135
Out Errors:	0
Last Connection:	172.19.229.50:28683

2. Select **On** to enable the query port server.
3. Click **Submit**.

Diagnostics

The MatchPort b/g Pro has several tools to perform diagnostics and view device statistics. These include information on:

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

Figure 12-17 Diagnostics: Hardware

The screenshot displays the 'Diagnostics: Hardware' page with the following sections and data:

Hardware	MIB-II	IP Sockets	
Ping	Traceroute	Log	Verbosity
Memory	Buffer Pools	Processes	

Diagnostics: Hardware

Current Configuration

CPU Type:	DSTnixFX
CPU Speed:	166.666666 MHz
CPU Instruction Cache:	4.000 Kbytes (4096 bytes)
CPU Data Cache:	4.000 Kbytes (4096 bytes)
RAM Size:	8.000000 Mbytes (8388608 bytes)
Flash Size:	8.000000 Mbytes (8388608 bytes)
Flash Sector Size:	64.000 Kbytes (65536 bytes)
Flash Sector Count:	128
Flash ID:	0x1

MIB-II Statistics

The MIB-II Network Statistics page shows the various SNMP-served Management Information Bases (MIBs) available on the MatchPort b/g Pro.

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.

Figure 12-18 MIB-II Network Statistics

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

Table 12-19 Requests for Comments (RFCs)

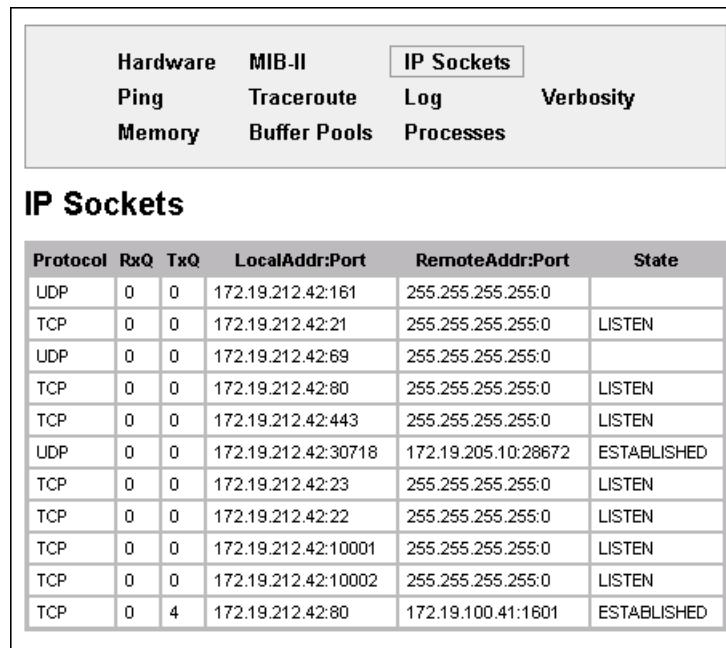
RFC 1213	Original MIB-II definitions.
RFC 2011	Updated definitions for IP and ICMP.
RFC 2012	Updated definitions for TCP.
RFC 2013	Updated definitions for UDP.
RFC 2096	Definitions for IP forwarding.

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 12-20 IP Sockets



The screenshot shows a user interface for managing network sockets. At the top, there is a navigation bar with tabs: Hardware, MIB-II, IP Sockets (which is selected and highlighted in a box), Ping, Traceroute, Log, Verbosity, Memory, Buffer Pools, and Processes. Below the navigation bar is a table titled "IP Sockets". The table has columns for Protocol, RxQ, TxQ, LocalAddr:Port, RemoteAddr:Port, and State. The data in the table is as follows:

Protocol	RxQ	TxQ	LocalAddr:Port	RemoteAddr:Port	State
UDP	0	0	172.19.212.42:161	255.255.255.255:0	
TCP	0	0	172.19.212.42:21	255.255.255.255:0	LISTEN
UDP	0	0	172.19.212.42:69	255.255.255.255:0	
TCP	0	0	172.19.212.42:80	255.255.255.255:0	LISTEN
TCP	0	0	172.19.212.42:443	255.255.255.255:0	LISTEN
UDP	0	0	172.19.212.42:30718	172.19.205.10:28672	ESTABLISHED
TCP	0	0	172.19.212.42:23	255.255.255.255:0	LISTEN
TCP	0	0	172.19.212.42:22	255.255.255.255:0	LISTEN
TCP	0	0	172.19.212.42:10001	255.255.255.255:0	LISTEN
TCP	0	0	172.19.212.42:10002	255.255.255.255:0	LISTEN
TCP	0	4	172.19.212.42:80	172.19.100.41:1601	ESTABLISHED

Ping

MatchPort b/g Pro 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.

Figure 12-21 Diagnostics: Ping

Diagnostics: Ping

Host:

Count:

Timeout: seconds

Submit

2. Enter or modify the following settings:

Table 12-22 Diagnostics: Ping

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

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

Traceroute

Here you can trace a packet from the MatchPort b/g Pro 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.

Figure 12-23 Diagnostics: Traceroute

Diagnostics: Traceroute

Host:

2. Enter or modify the following setting:

Table 12-24 Diagnostics: Traceroute

Diagnostics: Traceroute Settings	Description
Host	Enter the IP address or DNS hostname. This address is used to show the path between it and the device when issuing the traceroute command.

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.

Figure 12-25 Diagnostics: Log

Diagnostics: Log

Configuration

Output:

2. Select the **Output** type and select one of the following:
- Disable (default)
 - Filesystem
 - Line1

Figure 12-26 Diagnostics: Log (Filesystem)

The screenshot shows a configuration interface for 'Diagnostics: Log'. At the top, there is a navigation bar with tabs: Hardware, MIB-II, IP Sockets, Log (which is selected), and Verbosity. Below the navigation bar, there are several configuration options:

- Output:** Set to 'Filesystem'.
- Max Length:** Set to '50' Kbytes.
- Severity Level:** Set to 'Debug'.

A 'Submit' button is located at the bottom right of the configuration area.

Figure 12-27 Diagnostics: Log (Line 1)

The screenshot shows a configuration interface for 'Diagnostics: Log'. At the top, there is a navigation bar with tabs: Hardware, MIB-II, IP Sockets, Log (which is selected), and Verbosity. Below the navigation bar, there are several configuration options:

- Output:** Set to 'Line 1'.
- Severity Level:** Set to 'Debug'.

A 'Submit' button is located at the bottom right of the configuration area.

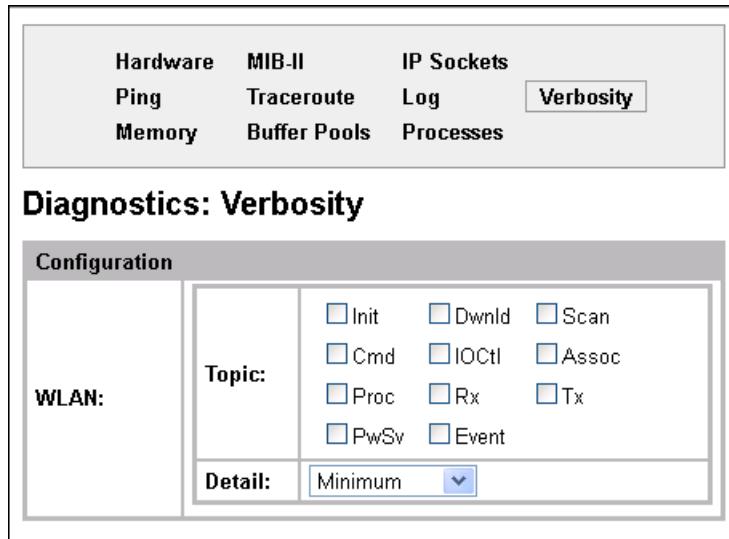
Verbosity

This page contains diagnostic verbosity configuration items. This controls which information shall be presented to log at the diagnostic level.

To configure the Verbosity:

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

Figure 12-28 Verbosity Configuration



2. Enter or modify the following settings:

Table 12-29 IP Address Filter Settings

IP Address Filter Settings	Description
Topic	Select the WLAN topics to be enabled for diagnostic logging.
Detail	Select the level of information or details to be logged regarding selected topics.

3. Click **Submit**.

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.

Figure 12-30 Diagnostics: Memory

Hardware	MIB-II	IP Sockets	
Ping	Traceroute	Log	Verbosity
Memory	Buffer Pools	Processes	
Diagnostics: Memory			
Main Heap			
Total Memory (bytes):	5677200		
Available Memory (bytes):	3435408		
Number Of Fragments:	4		
Largest Fragment Avail:	3421264		
Allocated Blocks:	2018		
Number Of Allocs Failed:	0		
Status	OK		

Buffer Pools

Several parts of the MatchPort b/g Pro 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.

Figure 12-31 Diagnostics: Buffer Pools

Hardware	MIB-II	IP Sockets		
Ping	Traceroute	Log	Verbosity	
Memory	Buffer Pools	Processes		
Diagnostics: Buffer pools				
Network Stack Buffer Pool				
Buffer Headers	Total 1024	Free 1021	Used 3	MaxUsed 11
Cluster Pool Size: 2048	512	509	3	9
Ethernet Driver Buffer Pool				
Buffer Headers	Total 512	Free 448	Used 64	MaxUsed 72
Cluster Pool Size: 2048	256	192	64	70

Processes

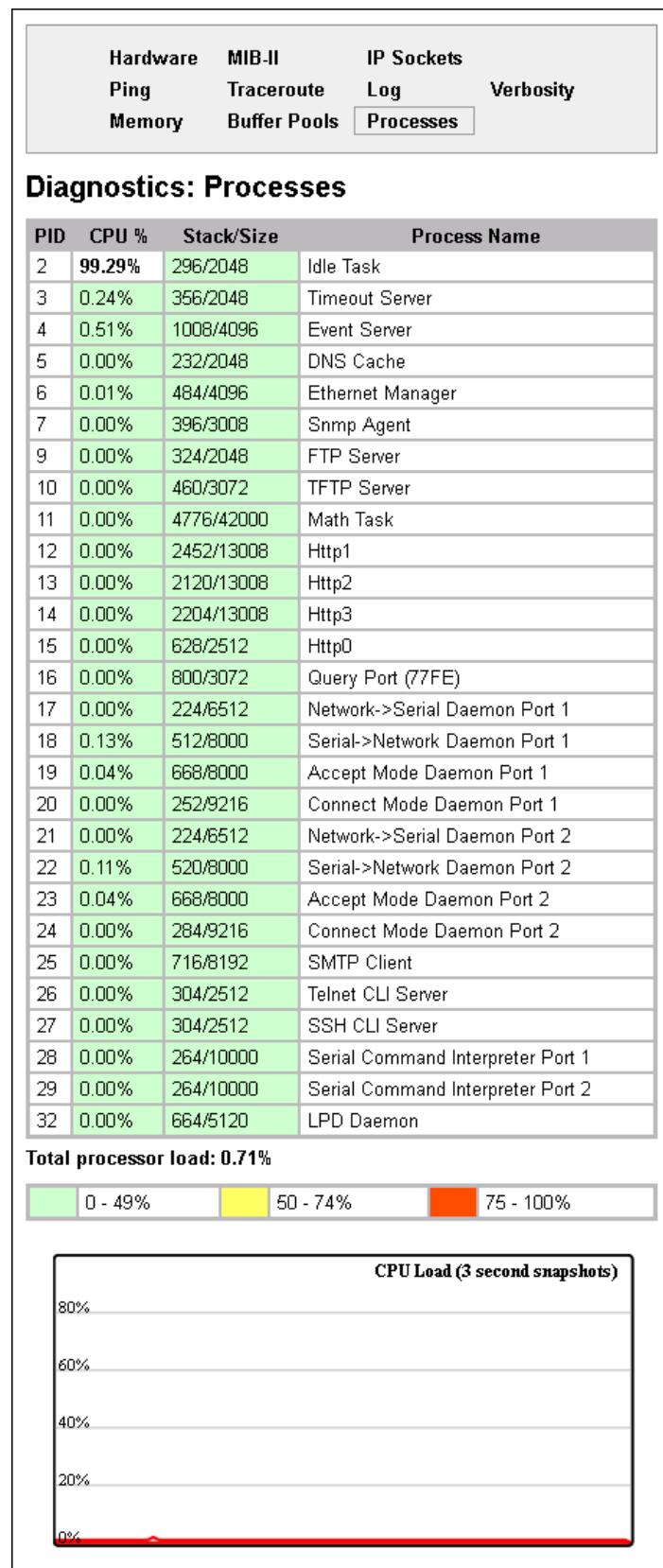
The Processes web page shows all the processes currently running on the system. It shows the Process ID (PID), the percentage of total CPU cycles a process used within the last three seconds, the total stack space available, the maximum amount of stack space used by the process since it started, and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

Figure 12-32 Diagnostics: Processes



System Settings

The MatchPort b/g Pro 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.

Figure 12-33 System

System	
Reboot Device	
<input type="button" value="Reboot"/>	
Restore Factory Defaults	
<input type="button" value="Factory Defaults"/>	
Upload New Firmware	
<input type="file"/>	<input type="button" value="Browse..."/>
<input type="button" value="Upload"/>	
Name	
Short Name:	<input type="text"/>
Long Name:	<input type="text"/>
<input type="button" value="Submit"/>	
Current Configuration	
Firmware Version:	5.2.0.0R12
Short Name:	my_device_server
Long Name:	Lantronix DeviceLinx

2. Configure the following settings:

Table 12-34 System

System Settings	Description
Reboot Device	Click Reboot to reboot the device. The system refreshes and redirects the browser to the device home page.
Restore Factory Defaults	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.

System Settings (continued)	Description
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 158 of Chapter 16: Branding the MatchPort b/g Pro .

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® b/g Pro allows you to view and configure email alerts relating to the events occurring within the system.

Please see [SMTP Settings on page 123](#) 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

The screenshot shows a web-based interface for managing email statistics. At the top, there are four tabs labeled "Email 1", "Email 2", "Email 3", and "Email 4". Below these are three sub-tabs: "Statistics", "Configuration", and "Send Email". The "Statistics" sub-tab is currently active for "Email 1".

The "Statistics" section contains a table with the following data:

Sent successfully:	1
Retries:	0
Not sent due to excessive errors:	0
In transmission queue:	0

Below the table is a "Log [Clear]" button. The log area displays a series of SMTP messages:

```
120:15:49 220 2putt.int.lantronix.com Microsoft ESMTP MAIL Service, Version: 6.0.3
120:15:49 EHLO eng.lantronix.com
120:15:49 250-2putt.int.lantronix.com Hello [172.19.100.129]
120:15:49 250-TURN
120:15:49 250-SIZE
120:15:49 250-ETRN
120:15:49 250-PIPELINING
120:15:49 250-DSN
120:15:49 250-ENHANCEDSTATUSCODES
120:15:49 250-8bitmime
120:15:49 250-BINARYMIME
120:15:49 250-CHUNKING
120:15:49 250-VRFY
120:15:49 250-X-EXPS GSSAPI NTLM LOGIN
120:15:49 250-X-EXPS=LOGIN
120:15:49 250-AUTH GSSAPI NTLM LOGIN
120:15:49 250-AUTH=LOGIN
120:15:49 250-X-LINK2STATE
120:15:49 250-XEXCH50
120:15:49 250 OK
120:15:49 MAIL FROM:<skuppuswamy@lantronix.com>
120:15:49 250 2.1.0 skuppuswamy@lantronix.com....Sender OK
120:15:49 RCPT TO:<skuppuswamy@lantronix.com>
120:15:49 250 2.1.5 skuppuswamy@lantronix.com
120:15:49 DATA
120:15:49 354 Start mail input; end with <CRLF>.<CRLF>
120:15:49 .
120:15:49 250 2.6.0
<2PUTTmopQeXr0kaK9Gt000002ac@2putt.int.lantronix.com> Queued
m
120:15:49 QUIT
```

Email Configuration

The MatchPort b/g Pro 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.

Figure 13-2 Email Configuration

Email 1 - Configuration	
To:	<input type="text"/>
CC:	<input type="text"/>
From:	<input type="text"/>
Reply To:	<input type="text"/>
Subject:	<input type="text"/>
Message File:	<input type="text"/>
Overriding Domain:	<input type="text"/>
Server Port:	25
Local Port:	<Random>
Priority:	<input type="radio"/> Urgent <input type="radio"/> High <input checked="" type="radio"/> Normal <input type="radio"/> Low <input type="radio"/> Very Low
Trigger Email Send:	CP Group: <input type="text" value="1"/> Value: <input type="text" value="0"/>
<input type="button" value="Submit"/>	

4. Enter or modify the following settings:

Table 13-3 Email Configuration

Email – Configuration Settings	Description
To	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.

Email – Configuration Settings (continued)	Description
CC	Enter the email address to which the email alerts will be copied. Multiple addresses are separated by semicolon (:).
From	Enter the email address to list in the From field of the email alert. Required field if an email is to be sent.
Reply-To	Enter the email address to list in the Reply-To field of the email alert.
Subject	Enter the subject for the email alert.
Message File	Enter the path of the file to send with the email alert. This file appears within the message body of the email.
Overriding Domain	Enter the domain name to override the current domain name in EHLO (Extended Hello).
Server Port	Enter the SMTP server port number. The default is port 25 .
Local Port	Enter the local port to use for email alerts. The default is a random port number.
Priority	Select the priority level for the email alert.
Trigger Email Send	Configure 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.

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:

1. Select **CLI** on the menu bar. The Command Line Interface Statistics page appears.

Figure 13-4 CLI Statistics

The screenshot displays the 'CLI Statistics' page with two main sections: 'Telnet' and 'SSH'. Both sections include fields for Server Status, Last Connection, Uptime, Total Bytes In, Total Bytes Out, and Current Connections. In the Telnet section, the status is 'Waiting' and uptime is '0 days 19:20:38'. In the SSH section, the status is also 'Waiting' and uptime is '0 days 19:20:38'.

Command Line Interface Statistics	
Telnet	
Server Status:	Waiting
Last Connection:	<None>
Uptime:	0 days 19:20:38
Total Bytes In:	0
Total Bytes Out:	0
Current Connections:	<None>
SSH	
Server Status:	Waiting
Last Connection:	<None>
Uptime:	0 days 19:20:38
Total Bytes In:	0
Total Bytes Out:	0
Current Connections:	<None>

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.

Figure 13-5 CLI Configuration

Command Line Interface Configuration	
Login Password:	<None>
Enable Level Password:	<None>
Quit Connect Line:	<control>L
Inactivity Timeout:	15 minutes
Telnet State:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Telnet Port:	23
Telnet Max Sessions:	3
SSH State:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
SSH Port:	22
SSH Max Sessions:	3

2. Enter or modify the following settings:

Table 13-6 CLI Configuration

Command Line Interface Configuration Settings	Description
Login Password	Enter the password for Telnet access.
Enable Level Password	Enter the password for access to the Command Mode Enable level. There is no password by default.
Quit Connect Line	Enter a string to terminate a connect line session and resume the CLI. Type <control> before any key the user must press when holding down the Ctrl key. An example of such a string is <control>L.
Inactivity Timeout	Set an Inactivity Timeout value so the CLI session will disconnect if no data is received after the designated time period. Default is 15 minutes. Enter a value of 0 to disable.
Telnet State	Select Disabled to disable Telnet access. Telnet is enabled by default.
Telnet Port	Enter the Telnet port to use for Telnet access. The default is 23 .
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 b/g Pro allows for the configuration of devices by using XML configuration records (XCRs). You can export an existing configuration for use on other MatchPort 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 b/g Pro 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>:<i>;<g>:<i>;...
```

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

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

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 embedded networking module, EDS8/16PS and EDS8/16/32PR) support additional lines.

Figure 13-7 XML: Export Configuration

XML: Export Configuration

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

To export the system configuration:

1. Select **XML** on the menu bar. The **XML: Export Configuration** 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 configuration vary between Lantronix products.

Export Configuration Export Status Import Configuration

XML: Export Configuration

Export to browser
 Export to local file
 Export secrets (use only with extreme caution) Comments

Lines to Export: [Clear All] [Select All]
 1 network

Groups to Export: [Clear All] [Select All but Networking]

<input checked="" type="checkbox"/> arp	<input checked="" type="checkbox"/> cli	<input checked="" type="checkbox"/> cp group
<input checked="" type="checkbox"/> device	<input checked="" type="checkbox"/> diagnostics	<input checked="" type="checkbox"/> email
<input checked="" type="checkbox"/> ethernet: eth0	<input checked="" type="checkbox"/> ftp server	<input checked="" type="checkbox"/> host
<input checked="" type="checkbox"/> http	<input checked="" type="checkbox"/> http server	<input checked="" type="checkbox"/> icmp
authentication uri	<input checked="" type="checkbox"/> ip	<input checked="" type="checkbox"/> ip filter
<input type="checkbox"/> interface: eth0	<input checked="" type="checkbox"/> lpd	<input checked="" type="checkbox"/> ManageLinx
<input checked="" type="checkbox"/> line	<input checked="" type="checkbox"/> ppp	<input checked="" type="checkbox"/> query port
<input checked="" type="checkbox"/> modbus	<input checked="" type="checkbox"/> serial command mode	<input checked="" type="checkbox"/> smtp
<input checked="" type="checkbox"/> rss	<input checked="" type="checkbox"/> ssh	<input checked="" type="checkbox"/> ssh client
<input checked="" type="checkbox"/> snmp	<input checked="" type="checkbox"/> ssl	<input checked="" type="checkbox"/> syslog
<input checked="" type="checkbox"/> ssh server	<input checked="" type="checkbox"/> telnet	<input checked="" type="checkbox"/> terminal
<input checked="" type="checkbox"/> tcp	<input checked="" type="checkbox"/> tunnel accept	<input checked="" type="checkbox"/> tunnel connect
<input checked="" type="checkbox"/> tftp server	<input checked="" type="checkbox"/> tunnel modem	<input checked="" type="checkbox"/> tunnel packing
<input checked="" type="checkbox"/> tunnel disconnect	<input checked="" type="checkbox"/> vip	<input checked="" type="checkbox"/> xml import control
<input checked="" type="checkbox"/> tunnel serial		

Export

Table 13-8 XML Export Configuration

XML Export Configuration Settings	Description
Export to browser	Select this option to export the XCR data in the selected fields to a web browser.
Export to local file	Select this option to export the XCR data to a file on the device. If you select this option, enter a file name for the XML configuration record.
Export secrets	Only use this with extreme caution. If selected, secret password and key information will be exported. Use only with a secure link, and save only in secure locations.
Lines to Export	Select the instances you want to export in the line, tunnel, and terminal groups.
Groups to Export	Check the configuration groups that are to be exported to the XML configuration record.

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.

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: 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.

Figure 13-9 XML: Export Status

Export Configuration **Export Status** Import Configuration

XML: Export Status

Export to browser
 Export to local file

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

1 network

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

<input checked="" type="checkbox"/> arp	<input checked="" type="checkbox"/> buffer pool	<input checked="" type="checkbox"/> cp group
<input checked="" type="checkbox"/> cps	<input checked="" type="checkbox"/> device	<input checked="" type="checkbox"/> email
<input checked="" type="checkbox"/> email log	<input checked="" type="checkbox"/> filesystem	<input checked="" type="checkbox"/> ftp
<input checked="" type="checkbox"/> hardware	<input checked="" type="checkbox"/> http	<input checked="" type="checkbox"/> http log
<input checked="" type="checkbox"/> icmp	<input checked="" type="checkbox"/> interface: eth0	<input checked="" type="checkbox"/> ip
<input checked="" type="checkbox"/> ip sockets	<input checked="" type="checkbox"/> line	<input checked="" type="checkbox"/> lpd
<input checked="" type="checkbox"/> memory	<input checked="" type="checkbox"/> modbus local slave	<input checked="" type="checkbox"/> modbus tcp server: additional
<input checked="" type="checkbox"/> modbus tcp server: permanent	<input checked="" type="checkbox"/> processes	<input checked="" type="checkbox"/> query port
<input checked="" type="checkbox"/> rss	<input checked="" type="checkbox"/> sessions	<input checked="" type="checkbox"/> ssh
<input checked="" type="checkbox"/> syslog	<input checked="" type="checkbox"/> tcp	<input checked="" type="checkbox"/> telnet
<input checked="" type="checkbox"/> tftp	<input checked="" type="checkbox"/> tunnel	<input checked="" type="checkbox"/> udp
<input checked="" type="checkbox"/> vip	<input checked="" type="checkbox"/> xsr	

Export

Table 13-10 XML Export Status

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

3. Click **Export**. The groups display if exporting 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.

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

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

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.

Figure 13-11 XML: Import Configuration

XML: Import Configuration

Import:

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

2. Click one of the following radio buttons:
 - Configuration from External file. *See Import Configuration from External File on page 145.*
 - Configuration from Filesystem. *See Import Configuration from the Filesystem on page 146.*
 - Line(s) from single line Settings on the Filesystem. *See Import Line(s) from Single Line Settings on the Filesystem on page 148.*

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.

Figure 13-12 XML: Import Configuration from External File

XML: Import Configuration

Import configuration from (entire) external XCR file:

Import

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

The screenshot displays a web-based configuration interface for importing XML files. At the top, there are three tabs: 'Export Configuration', 'Export Status', and 'Import Configuration', with 'Import Configuration' being the active tab. Below the tabs, the title 'XML: Import Configuration' is centered. A sub-section titled 'Import configuration from the filesystem:' contains a 'Filename' input field. Underneath it, 'Lines to Import' offers '[Clear All]' and '[Select All]' buttons, with a single checkbox selected for line '1' and another for 'network'. A large section labeled 'Whole Groups to Import' includes '[Clear All]' and '[Select All but Networking]' buttons, followed by a grid of checkboxes for various configuration groups. The groups listed are: arp, cli, cp group; device, diagnostics, email; ethernet, execute, exit cli; ftp server, host, http authentication uri; http server, icmp, interface; ip, ip filter, line; lpd, ManageLinx, modbus; ppp, query port, rss; serial command mode, smtp, snmp; ssh, ssh client, ssh server; ssl, syslog, tcp; telnet, terminal, tftp server; tunnel accept, tunnel connect, tunnel disconnect; tunnel modem, tunnel packing, tunnel serial; and vip, xml import control. At the bottom, there is a 'Text List' input field and a prominent blue 'Import' button.

1. Enter or modify the following settings.

Figure 13-14 XML: Import Configuration from Filesystem

Import Configuration from Filesystem Settings	Description
Filename	Enter the name of the file on the device (local to its filesystem) that contains XCR data.
Lines to Import	Select the lines or network whose settings you want to import. Click the Select All link to select all the serial lines and the network lines. Click the Clear All link to clear all of the checkboxes. By default, all line instances are selected. Only the selected line instances will be imported in the line, tunnel, and terminal groups.
Whole Groups to Import	Select the configuration groups to import from the XML configuration record. This option imports all instances of each selected group unless it is one of the Lines to Import . Note: <i>By default, all groups are checked except those pertaining to the network configuration; this is so that import will not break your network connectivity.</i> You may check or uncheck any group to include or omit that group from import. To import all of the groups, click the Select All but Networking link to import all groups. To clear all the checkboxes, click the Clear All link.
Text List	Enter a string to import specific instances of a group. The textual format of this string is: <g>:<i>;<g>:<i>;... Each group name <g> is followed by a colon and the instance value <i> and each <g>:<i> value is separated by a semi-colon. If a group has no instance, then specify the group name <g> only. Use this option for groups other than those affected by Lines to Import .

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

The screenshot shows a software interface titled "XML: Import Configuration". At the top, there are three tabs: "Export Configuration", "Export Status", and "Import Configuration", with "Import Configuration" being the active tab. Below the tabs, the title "XML: Import Configuration" is centered. The main area contains the following sections:

- Import Line(s) from single line settings on the filesystem:**
 - Filename: A text input field.
 - Lines to Import: Buttons for "[Clear All]" and "[Select All]". Below these are two checkboxes: 1 and network.
- Whole Groups to Import:** Buttons for "[Clear All]" and "[Select All but Networking]". Below these are two columns of checkboxes:

<input checked="" type="checkbox"/> arp	<input checked="" type="checkbox"/> cli	<input checked="" type="checkbox"/> cp group
<input checked="" type="checkbox"/> device	<input checked="" type="checkbox"/> diagnostics	<input checked="" type="checkbox"/> email
<input checked="" type="checkbox"/> ethernet	<input checked="" type="checkbox"/> execute	<input checked="" type="checkbox"/> exit cli
<input checked="" type="checkbox"/> ftp server	<input checked="" type="checkbox"/> host	<input checked="" type="checkbox"/> http authentication uri
<input checked="" type="checkbox"/> http server	<input checked="" type="checkbox"/> icmp	<input type="checkbox"/> interface
<input checked="" type="checkbox"/> ip	<input checked="" type="checkbox"/> ip filter	<input checked="" type="checkbox"/> line
<input checked="" type="checkbox"/> lpd	<input checked="" type="checkbox"/> ManageLinx	<input checked="" type="checkbox"/> modbus
<input checked="" type="checkbox"/> ppp	<input checked="" type="checkbox"/> query port	<input checked="" type="checkbox"/> rss
<input checked="" type="checkbox"/> serial command mode	<input checked="" type="checkbox"/> smtp	<input checked="" type="checkbox"/> snmp
<input checked="" type="checkbox"/> ssh	<input checked="" type="checkbox"/> ssh client	<input checked="" type="checkbox"/> ssh server
<input checked="" type="checkbox"/> ssl	<input checked="" type="checkbox"/> syslog	<input checked="" type="checkbox"/> tcp
<input checked="" type="checkbox"/> telnet	<input checked="" type="checkbox"/> terminal	<input checked="" type="checkbox"/> tftp server
<input checked="" type="checkbox"/> tunnel accept	<input checked="" type="checkbox"/> tunnel connect	<input checked="" type="checkbox"/> tunnel disconnect
<input checked="" type="checkbox"/> tunnel modem	<input checked="" type="checkbox"/> tunnel packing	<input checked="" type="checkbox"/> tunnel serial
<input checked="" type="checkbox"/> vip	<input checked="" type="checkbox"/> xml import control	

At the bottom left is a blue "Import" button.

- Enter or modify the following settings:

Table 13-16 XML: Import Line(s) from Single Line Settings

Import Line(s) Settings	Description
Filename	Provide the name of the file on the device (local to its file system) that contains XCR data.
Lines to Import	Select the line(s) whose settings you want to import. Click the Select All link to select all the serial lines and the network lines. Click the Clear All link clear all of the checkboxes. By default, all serial line instances are selected.
Whole Groups to Import	Select the configuration groups to import from the XML configuration record. Note: <i>By default, all groups are checked except those pertaining to the network configuration; this is so that import will not break your network connectivity.</i> 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.

- Click **Import**.

CPU Power Management

This web page allows you to configure CPU power management, specifically the power management of the cpu, the on-chip peripherals and the extended memory.

To enable or disable CPU power:

- Click **CPU Power Mgmt** on the menu bar. The CPU Power Management page appears.

Figure 13-17 CPU Power Management



- Enter or modify the following settings:

Table 13-18 Modbus Configuration

CPU Power Management Configuration Settings	Description
State	Click to enable or disable CPU Power Management: ◆ Enabled ◆ Disabled

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

14: Bridging

The MatchPort® b/g Pro embedded device server supports bridging of traffic between a single external Ethernet device and the wireless network. When bridging is enabled and active, the MAC address of the external device is used as the MAC address for the WLAN interface. The MatchPort b/g Pro then bridges traffic between the two interfaces. The external Ethernet device appears as a wireless node on the network.

When bridging is enabled, the concept of the Primary Interface is introduced. The Primary Interface is the interface over which all MatchPort b/g Pro features and services operate, as if bridging were not enabled. FTP, Telnet CLI, HTTP, 77FE, etc, all may be accessed as usual over the Primary Interface. The Primary Interface dynamically switches between eth0 and wlan0, depending on the state of the Ethernet physical link. If the Ethernet link is up, eth0 is the Primary Interface; otherwise, wlan0 is the Primary Interface.

When bridging is enabled, operation of Network 1 (eth0) and Network 2 (wlan0) are overridden and controlled by the bridging subsystem. The Primary Interface always uses the Network 1 (eth0) Interface Configuration (see [Network 1 \(eth0\) Interface Configuration](#)) for its settings. Network 2 (wlan0) Interface Configuration is ignored when bridging is enabled. Network 1 (eth0) and Network 2 (wlan0) Link Configuration settings are still used to configure and control the physical links.

Bridging Configuration

To configure and enable bridging, follow these guidelines:

1. Configure Network 1 (eth0) Interface settings, which will be used for the Primary Interface. For example,
 - DHCP Disabled
 - IP Address 192.168.1.100/24
 - Default Gateway 192.168.1.1
2. Configure Network 1 (eth0) Link settings, if desired. These include the Ethernet link speed and duplex.
3. Configure Network 2 (wlan0) Link settings as desired for connection to a wireless network. Primarily, configure the WLAN Profile(s) for connection to the wireless network.
4. Create the corresponding WLAN Profile(s) under the WLAN Profiles page.

At this point, it is a good idea to ensure that the MatchPort b/g Pro can connect to your wireless network, before enabling bridging. Check your WLAN settings by continuing with the following steps:

5. Enable Network 2 (wlan0) and Disable Network 1 (eth0).
6. Configure Network 2 (wlan0) Interface settings as desired.
7. Reboot.
8. Verify the wireless connection.
9. Enable Bridge 1 (bridge0).
10. Optionally configure the Bridge 1 Bridging MAC Address.
11. Reboot for changes to take effect.

Bridging Operation

During initialization, both eth0 and wlan0 are enabled and controlled by the bridging subsystem. Important aspects to keep in mind:

- ◆ eth0 always uses the MatchPort b/g Pro's factory-configured MAC Address
- ◆ If eth0 physical link is down, wlan0 uses the MatchPort b/g Pro's factory-configured MAC address and wlan0 is the Primary Interface.
- ◆ If eth0 physical link is up, wlan0 uses the Bridging MAC Address (either pre-configured or auto-detected), and eth0 is the Primary Interface.

When eth0 link is up, wlan0 link is established, and the Bridging MAC Address is acquired (via pre-configuration or auto-detection), Bridging enters the Active state. If either link goes down, bridging falls back to the Inactive state.

When in the Active state, all packets that arrive on the wlan0 interface are bridged out the eth0 interface. Similarly, all packets that arrive on the eth0 interface are bridged out the wlan0 interface. However, exceptions to this behavior include:

- ◆ Ethernet packets directed specifically to the Ethernet MAC Address are terminated internally and are not bridged to WLAN.
- ◆ ARP Requests for the Primary Interface's IP address are terminated internally and are not bridged to WLAN
- ◆ Ethernet packets which are not originated from the Bridging MAC Address are discarded.

Bridge Settings

A bridge may be configured between an Ethernet interface and a WLAN interface. A bridge represents a relationship between the interface minor numbers. For example, br0 is a bridge between eth0 and wlan0.

Bridge 1 (bridge0) Status

This page shows the status of the Ethernet-to-WLAN network bridge.

To view the bridge status:

1. Click **Bridge** on the menu.
2. Then click **Status** at the top of the page. The Bridge 1 (bridge0) Status page appears.

Figure 14-1 Bridge 1 (bridge0) Status

Bridge 1		
Status Configuration		
Bridge 1 (bridge0) Status		
Enable State:	Disabled	
Active State:	Inactive	
Ethernet Link:	N/A	
WLAN Link:	N/A	
Primary Interface:	N/A	
Bridging MAC:	N/A	
Ethernet MAC:	N/A	
WLAN MAC:	N/A	
Statistics	Ethernet to WLAN	WLAN to Ethernet
Unicast:	0	0
NonUnicast:	0	0
Discards:	0	0
Octets:	0	0

Table 14-2 Status Page Items:

Bridge 1 Status Page Items	Description
Enable State	Enable State of the network bridge. <ul style="list-style-type: none"> ◆ Enabled = the bridge is enabled. ◆ Disabled = the bridge is disabled. <p>Note: If the bridge is enabled or disabled from the Configuration page, it will not actually be charged until after a reboot. When the bridge state is Enabled, Network Interface settings for the eth0 interface are used for the Primary Interface. wlan0 Network Interface settings are ignored.</p>
Active State	Active State of the network bridge. <ul style="list-style-type: none"> ◆ Active = the bridge is active. Received packets are being bridged across the two interfaces. ◆ Inactive = the bridge is inactive.
Ethernet Link	Current state of the Ethernet Physical link. <p>This is the same format that appears on the main Status page when Network 1 (eth0) is active. Format string shows the current configuration, followed by the link state in parentheses.</p>
WLAN Link	Current state of the WLAN Physical link. <p>This is the same format that appears on the main Status page when Network 2 (wlan0) is active. Displayed is the current link state – “ESTABLISHED” or “not established”. More detail on the state of the physical link can be found on the Network 2 (wlan0) Link Status page.</p>

Bridge 1 Status Page Items	Description
Primary Interface	<p>The current Primary Interface (eth0 or wlan0). The Primary Interface is the interface which is currently terminating traffic directed internally to the MatchPort b/g Pro. All normal, non-bridging communications over this interface will be handled properly, such as web access, telnet access, etc.</p> <p>The Primary Interface switches dynamically. When the Network 1 (eth0) link is physically connected, then it is the Primary Interface. If the eth0 link is down, then Network 2 (wlan0) becomes the Primary Interface.</p>
Bridging MAC	<p>The MAC address of the external Ethernet device, whose traffic is being bridged to/from the wireless network. If the Bridging MAC Address is not pre-configured, and if the first packet has not been received over the Ethernet interface, then this field will display as "Not Acquired".</p>
Ethernet MAC	<p>The MAC address of the internal Ethernet interface (eth0). This is the MatchPort b/g Pro's factory-configured MAC address.</p>
WLAN MAC	<p>The MAC address of the internal WLAN interface (wlan0). This address dynamically switches between the Bridging MAC and the Ethernet MAC, depending on the state of the bridge. If wlan0 is the Primary Interface (eth0 link is down), then this is the same as the Ethernet MAC. If bridge0 is Active, this is the same as the Bridging MAC Address.</p>
Unicast Statistics	<p>These statistics reflect the number of Ethernet Unicast packets that have been bridged between the two interfaces.</p>
NonUnicast Statistics	<p>These statistics reflect the number of Ethernet NonUnicast packets that have been bridged between the two interfaces.</p>
Discards Statistics	<p>These statistics reflect the number of Ethernet packets which have been discarded because the source address does not match the Bridging MAC Address.</p>
Octets Statistics	<p>These statistics reflect the number of octets which have been bridged between the two interfaces.</p>

Bridge 1 (bridge0) Configuration

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

To view and configure bridge settings:

1. Click **Configuration** at the top of the page. The Bridge 1 (bridge0) Configuration page appears.

Figure 14-3 Bridge 1 (bridge0) Configuration

2. Enter or modify the following settings:

Bridge 1 Configuration Page Settings		Description
State	State of the network bridge. ◆ Enabled = the bridge is enabled. ◆ Disabled = the bridge is disabled. Note: A reboot is required for any change to take effect. When the bridge is Enabled, Network Interface settings for the eth0 interface are used for the Primary Interface. wlan0 Network Interface settings are ignored.	
Bridging MAC Address	Enter the MAC address of the external Ethernet device which is to be bridged to/from the wireless network. If this field is left empty, then the MatchPort b/g Pro will wait for the first received Ethernet packet to detect and configure the Bridging MAC Address. Note: A reboot is required for any change to take effect. A Bridging MAC Address that is auto-detected will not survive a reboot. Auto-detected addresses are not saved in the configuration.	

3. To save changes, click **Submit**. Changing any of these settings requires a reboot to take effect.

15: 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® b/g Pro make use of SSL. The MatchPort® b/g Pro embedded device server 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 b/g Pro will use its own "personal" certificate. In verifying the authenticity of the other party, the MatchPort b/g Pro will use a "trusted authority" certificate.

In short:

- ◆ When using EAP-TLS, the MatchPort b/g Pro needs a personal certificate with matching private key to identify itself and sign its messages.
- ◆ When using EAP-TLS, EAP-TTLS or PEAP, the MatchPort b/g Pro needs the authority certificate(s) that can authenticate those it wishes to communicate with.

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 b/g Pro 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 b/g Pro.

Certificate Formats

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. Additionally, the key can be either be encrypted with a password or left in the clear. However, the MatchPort b/g Pro 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:

```
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.

Steel Belted RADIUS

Steel Belted RADIUS is a commercial RADIUS server from Juniper Networks that provides a GUI administration interface. It also provides a certificate request and self-signed certificate generator.

The self-signed certificate has extension `.sbrpvk` and is in the PKCS12 format. OpenSSL can convert this into a PEM format certificate and key:

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

The `sbr_certkey.pem` file contains both certificate and key. If loading the SBR certificate into MatchPort b/g Pro as an authority, you will need to edit it:

1. Open the file in any plain text editor.
2. Delete all info before "----- BEGIN CERTIFICATE-----" and after "----- END CERTIFICATE-----", and then save as `sbr_cert.pem`.

SBR accepts trusted-root certificates in the DER format. Again, OpenSSL can convert any format into DER:

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

Note: With SBR, when the identity information includes special characters such as dashes and periods, SBR changes the format it uses to store these strings and becomes incompatible with the current MatchPort b/g Pro release. Support may be added for this and other formats in future releases.

Free RADIUS

Free RADIUS is another versatile Linux open-source RADIUS server.

16: Branding the MatchPort b/g Pro

This chapter describes how to brand your MatchPort® b/g Pro 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 MatchPort b/g Pro embedded device server file system.

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

1. FTP to the MatchPort b/g Pro 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 b/g Pro (MatchPort b/g Pro)
```

17: 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:

1. Select **System** in the menu bar. The **Filesystem** page appears.

Figure 17-1 Update Firmware

The screenshot shows the 'System' configuration page. It includes sections for 'Reboot Device' (with a 'Reboot' button), 'Restore Factory Defaults' (with a 'Factory Defaults' button), and 'Upload New Firmware'. The 'Upload New Firmware' section contains a file input field with a 'Browse...' button, an 'Upload' button, and fields for 'Name', 'Short Name', and 'Long Name' with a 'Submit' button. A red circle highlights the 'Upload New Firmware' section.

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® b/g Pro. 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 b/g Pro 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:

Technical Support US

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

Technical Support Europe, Middle East, Africa

Phone: +33 13 930 4172

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

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

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

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

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® b/g Pro Embedded Device Server

Conform to the following standards or other normative documents:

Radiated and Conducted Emissions

EMC & Radio:

For purposes of certification, the MatchPort b/g pro was tested as a modular device.

CFR Title 47 FCC Part 15, Subpart B and C, Class B

FCC Module Approval

FCC Identifier: R68MPBGP0

Industry Canada ICES-003 Issue 4 (2004), Class B

Industry Canada RSS-Gen Issue 2 (2007)

Industry Canada RSS-210 Issue 7 (2007)

Industry Canada Module Approval IC: 3867A-MPBGP0

EN 301 489-1 v1.6.1 (2006-07), EMC Directive (1999/5/EC)

EN 301 489-17 v.1.2.1 (2002-08), EMC Directive (1999/5/EC)

EN 300 328 v1.7.1 (2006-10), R&TTE Directive (1999/5/EC)

Australia / New Zealand AS/NZS CISPR 22 (2006), Class B

Australia / New Zealand AS/NZS 4771 (2000 + A1:2003)

EN55022: 2006

EN55024: 1998 + A1: 2001 + A2: 2003

EN61000-3-2: 2006

EN61000-3-3: 1995 + A1: 2001

Safety

UL 60950-1

CAN/CSA-C22.2 No. 60950-1-03

EN 60950-1:2006, Low Voltage Directive (73/23/EEC)

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:

◆ Lead (Pb)	◆ Mercury (Hg)				◆ Polybrominated biphenyls (PBB)	◆ Polybrominated diphenyl ethers (PBDE)
◆ Cadmium (Cd)	◆ Hexavalent Chromium (Cr (VI))					
Product Family Name	Toxic or hazardous Substances and Elements					
	Lead (Pb)	Mercury (Hg)	Cadmium (Cd)	Hexavalent Chromium (Cr (VI))	Polybrominated biphenyls (PBB)	Polybrominated diphenyl ethers (PBDE)
UDS1100 and 2100	0	0	0	0	0	0
EDS	0	0	0	0	0	0
MSS100	0	0	0	0	0	0
IntelliBox	0	0	0	0	0	0
XPress DR & XPress-DR+	0	0	0	0	0	0
SecureBox 1101 & 2101	0	0	0	0	0	0
WiBox	0	0	0	0	0	0
UBox	0	0	0	0	0	0
MatchPort	0	0	0	0	0	0
SLC	0	0	0	0	0	0
XPort	0	0	0	0	0	0
WiPort	0	0	0	0	0	0
SLB	0	0	0	0	0	0
SLP	0	0	0	0	0	0
SCS	0	0	0	0	0	0
SLS	0	0	0	0	0	0
DSC	0	0	0	0	0	0
PremierWave	0	0	0	0	0	0
Micro125	0	0	0	0	0	0

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.

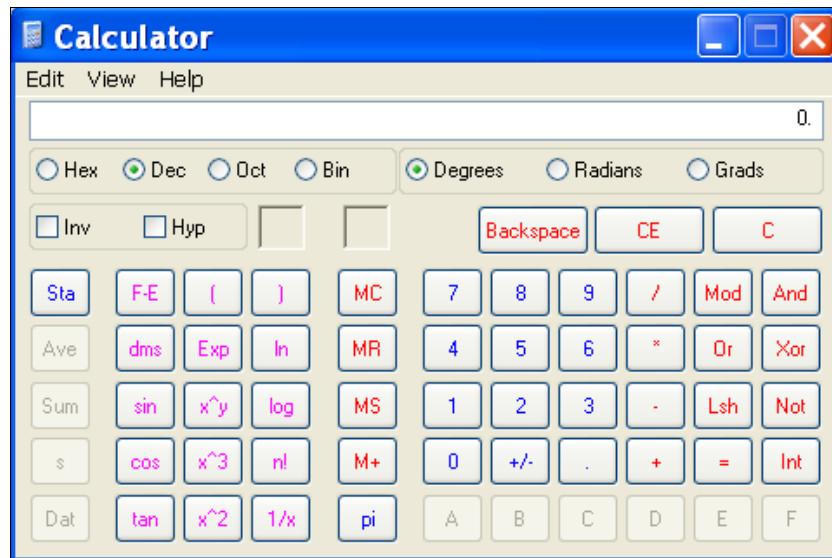
Table C-1 Binary to Hexadecimal Conversion Table

Decimal	Binary	Hex
0	0000	0
1	0001	1
2	0010	2
3	0011	3
4	0100	4
5	0101	5
6	0110	6
7	0111	7
8	1000	8
9	1001	9
10	1010	A
11	1011	B
12	1100	C
13	1101	D
14	1110	E
15	1111	F

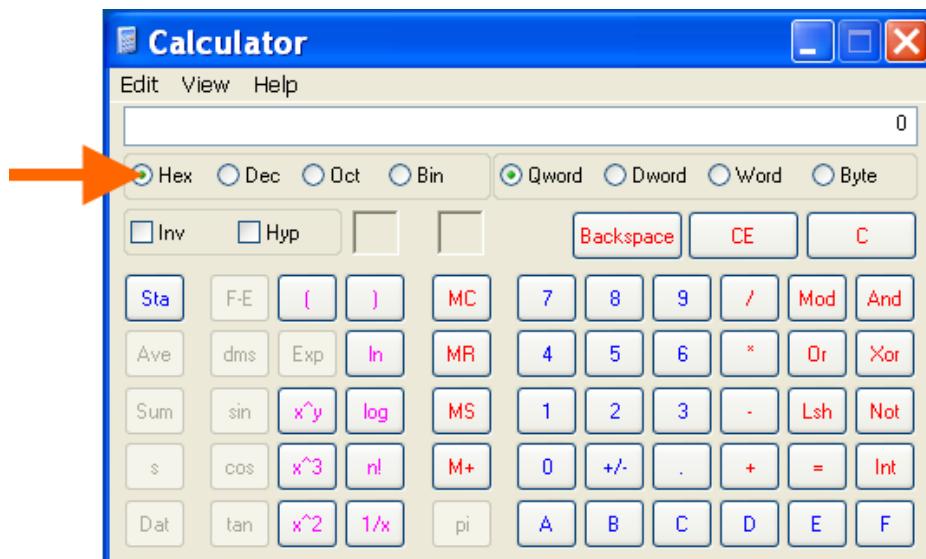
Scientific Calculator

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.



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



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 49
Accept Mode 55
Additional Documentation 14
Additional TCP Server Port 115
Address
 Ethernet 19
 Hardware 19, 20
 IP 19
 MAC 19, 20
Advanced Settings
 Email Configuration 138
 XML Configuration 142
Advanced Settings 137
AES 16
Allow Firmware Update 84
Allow TFTP File Creation 84
Allow XCR Import 84
ARP 16
ARP Settings 122, 123
ASCII 111
Auth Type 90
Authentication Mode 80
Authentication Type 90
Authority 109
AutoIP 16

B

Banner 93
Bar Code 20
Bin 164
Binary 73, 93, 163
Binary to Hexadecimal Conversions 163
Bit 73, 76
Block Network 57, 61
Block Serial 61
Block Serial Data 57
BOOTP 16, 30, 33
Branding 158
 Web Manager Customization 158
Break Duration 68

C

Challenge Handshake Authentication Protocol 79
CHAP 79

CLI 17
CLI Configuration 140
CLI Statistics 140
Command Line Interface Settings 140
Command Mode 19
Command-Line Interface 17
Common Name 110
Compliance 161
Configurable Pin Manager 71
Configuration Methods 18
Configuration Settings 78
Configured As 73
Connect Mode 49
Connect Mode 58
Connection Value 57
Convert Newlines 94
Count 129
CP 73
CP Output 57, 61
CPM 71
Create New Keys 104
Create New Self-Signed Certificate 109
Custom Groups 71

D

Default Gateway 30, 34
Default Groups 71
Default Server Port Numbers 19
Device Control 17
Device Details 21
Device Details Summary 21
Device Management 18
Device Status 24
DeviceInstaller 21
DeviceInstaller 21
DHCP 16, 30, 33
Diagnostic Toolset 18
Diagnostics 126
 Buffer Pools 133
 Hardware 126
 IP Sockets 128
 Memory 132
 MIB-II Statistics 127
 Ping 128
 Processes 134
Diagnostics Log 130
Diagnostics Settings 116
Direct & Indirect ESD 161
Disconnect Mode 49
Disconnect Mode 62
Disconnection Value 57
DNS 16, 30, 34

DNS Settings 78

E

Echo 68, 69
Email on Connect 57, 61
Email on Disconnect 57, 61
Enable Level Password 141
Encryption 18
End of Job 93
Enterprise-Grade Security 17
EOJ String 94
Ethernet address 19
Evolution OS 16
Evolution OS™ 16
Exit Connect Menu 68, 69
Expires 110
Export Secrets 143
Export to Browser 143, 144
Export to Local File 143, 144

F

File System

Browser 117
Statistics 116
Filename 147, 149
Filesystem 26, 159
Firmware 159
Flush Serial Data 57, 61
Formfeed 94
FreeRADIUS 107
FTP 16, 159
FTP Configuration 82

G

Groups to Export 143, 144

H

Hardware Address 19, 20
Hardware Address 19
Help Area 25
Hex 164
Hexadecimal 163
Host 60, 118, 129, 130
Host Configuration 69
Host Configuration 69

Host IP Promotion 62

Hostname 30, 34

HTTP 16

 Authentication 89
 Change Configuration 87
 Configuration 86
 Statistics 86

I

I/O 73
ICMP 16
ICMP Settings 121
Import Configuration from External File 145
Import Configuration from the Filesystem 146
Import Line(s) from Single Line Settings on the File-system 148
Inactivity Timeout 141
IP 16
 Address 19
 Address Filter 124, 132
 Settings 120
ISO/IEC Guide 161

K

Key Features 15
Key Length 110
Key Type 97, 98, 104

L

Label 20
Lantronix Discovery Protocol 19
Level 73
Line 1
 Configuration 46
 Statistics 45
Line Settings 45
Lines to Export 143, 144
Lines to Import 147, 149
Loading New Firmware 159
Local IP Address 80
Local Port 57, 60
Logic 73
Login Connect Menu 68, 69
Login Password 141
Logout 25
LPD
 Configuration Page 93

Settings 92
LPD Statistics 92

M

MAC Address 19, 20
Maintenance and Diagnostics Settings
 Protocol Stack 119
Maintenance Settings 116
Manufacturer's Contact 161
Manufacturer's Name & Address 161
Max Entries 91
Modbus Configuration 115
Modbus Statistics 114
Modbus 111
Modbus_Ctl_In 111
Modbus_Ctl_Out 111
Mode 60
Modem Emulation 17
Modem Emulation 64
MTU 30, 34
Multiple Hosts 62

PBX 18
Peer IP Address 80
Persistent 91
Point-to-Point Protocol 79
Port 118
Port Numbers 19
Ports
 Serial and Telnet 19
PPP Peer Device 79
PPP Settings 79
Private Branch Exchange 18
Private Key 97, 98, 104
Product Information Label 20
Product Name Model 161
Product Revision 20
Protocol 57, 70
Protocol Support 16
Public Key 97, 98, 104

Q

Query Port 125
Queue Name 94
Quit Connect Line 141

N

Name 136
NAT 79
Network 1 (eth0) Interface Configuration 29
Network 1 Ethernet Link 31
Network Address Translation 79
Network Settings
 Network 1 Interface Configuration 29, 32, 35,
 154
 Network 1 Interface Status 28, 32, 34, 151
Network Settings 28
New Certificate 109
New Private Key 109

Radiated and Conducted Emissions 161
Read Community 82
Really Simple Syndication 17
Reboot Device 135
Reconnect Timer 61
Ref 73
Remote Address 70
Remote Command 104
Remote Port 70
Response Timeout 115
Restore Factory Defaults 135
RFC1334 79
RoHS Notice 162
RSS 16, 17
RSS Feed 91
RSS Settings 91
RSS Trace Input 115
RTU 111

O

Obtaining Firmware 159
Organization Unit 109

Packing Mode 53
PAP 79
Password 57, 81, 104
Password Authentication Protocol 79

S
Scientific 164
Scientific Calculator 164

SCPR 18	System Settings 135
Secure Com Port Redirector 18	
Secure Shell 95	
Secure Sockets Layer 95, 105	
Security	
Enterprise-Grade 17	TCP 16
Settings 95	TCP Keep Alive 57
Security Settings 95	TCP Server State 115
SSL Certificates and Private Keys 106	TCP Settings 119
SSL Cipher Suites 105	TCP/IP 111
SSL RSA or DSA 106	Technical Support 160
SSL Utilities 107	Telnet 16
Send Break 68	Telnet Max Sessions 141
Send Character 55	Telnet Port 141
Serial Settings 52	Telnet State 141
Serial Transmission Mode 113	Terminal
Services Settings 78	Server 18
CHAP Authentication 79	Settings 67
LPD 92	Terminal Type 68, 69
Short and Long Name Customization 158	Text List 147
SMTP 16	TFTP 16, 159
SNMP 16	TFTP Configuration 83
SNMP Configuration 81	Threshold 55
SNMP Management 17	Timeout 55, 129
SOJ String 94	TLS 16
SSH 16, 95	Traceroute 129
Client Known Hosts 102	Trailing Character 55
Server Authorized Users 100	Traps Primary Destination 82
Server Host Keys 96	Traps Secondary Destination 82
Settings 95	Traps State 82
SSH Client Known Hosts 102	Troubleshooting 18
SSH Client User Configuration 103	Troubleshooting Capabilities 18
SSH Max Sessions 141	Tunnel – Accept Mode 55
SSH Port 141	Tunnel – Connect Mode 58
SSH Server Authorized Users 100	Tunnel – Disconnect Mode 62
SSH Server Host Keys 96	Tunnel – Packing Mode 53
SSH State 141	Tunnel 1 – Statistics 50
SSH Username 70	Tunnel Settings
SSL 16, 95, 105	Connect Mode 58
Settings 105	Modem Emulation
SSL Certificates 106	Command Mode 64
SSL Cipher Suites 105	Packing Mode 53
SSL Configuration 108	Tunnel Settings 49
SSL RSA or DSA 106	Type 110
SSL Utilities 107	
Start of Job 93	
State 121	
Steel Belted RADIUS 107	
Syslog 16	U
Syslog Configuration 84	UDP 16
System Contact 82	Uniform Resource Identifier 89
System Description 82	Updating Firmware 159
System Location 82	Upload Authority Certificate 109
System Name 82	Upload Certificate 109

Upload New Firmware 136

URI 89

Username 81, 104

W

Web Manager

Device Status Web Page 24

Navigating 26

Page Components 25

Page Summary 26

Web Manager Customization 158

Web Manager 23

Web-Based Configuration 17

Whole Groups to Import 147, 149

WLAN

Authentication 43

Profiles

create or delete 38

Settings

Network 1 Ethernet Link 31

WEP Settings 40

WPA 41, 43

WPA2/IEEE802.11i 41, 43

Write Community 82

X

XML 19

Export Configuration 143

Export Status 144

Import System Configuration 145

XML-Based Architecture 17