

LANTRONIX®

# MatchPort® b/g Pro



## MatchPort b/g Pro User Guide

Part Number 900-531  
Revision A April 2008

## Copyright & Trademark

© 2008 Lantronix. All rights reserved. No part of the contents of this book may be transmitted or reproduced in any form or by any means without the written permission of Lantronix. Printed in the United States of America.

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

## Contacts

### Lantronix Corporate Headquarters

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

### Technical Support

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

### Sales Offices

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

## Disclaimer & Revisions

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

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

Date	Rev.	Comments
April 2008	A	Initial Document

# Contents

Figures	7
<b>1: Using This Guide</b>	<b>9</b>
Purpose and Audience	9
Summary of Chapters	9
Additional Documentation	10
<b>2: Introduction</b>	<b>11</b>
Key Features	11
Applications	11
Protocol Support	12
Evolution OS™	12
Additional Features	12
Modem Emulation	12
Web-Based Configuration and Troubleshooting	13
Command-Line Interface (CLI)	13
SNMP Management	13
XML-Based Architecture and Device Control	13
Really Simple Syndication (RSS)	13
Enterprise-Grade Security	13
Terminal Server/Device Management	14
Troubleshooting Capabilities	14
Configuration Methods	15
Addresses and Port Numbers	15
Hardware Address	15
IP Address	15
Port Numbers	15
Product Information Label	16
<b>3: Using DeviceInstaller</b>	<b>17</b>
Accessing MatchPort b/g Pro using DeviceInstaller	17
Viewing the MatchPort b/g Pro's Current Configuration	17
<b>4: Configuration Using Web Manager</b>	<b>20</b>
Accessing Web Manager Through a Web Browser	20
Understanding the Web Manager Pages	22
Navigating Through the Web Manager	23

Device Status Page	33
<b>5: Network Settings</b>	<b>34</b>
Network Settings	34
Network 1 (eth0) Interface Status	34
Network 1 (eth0) Interface Configuration	35
Network 1 Ethernet Link	37
WLAN Settings	38
Network 2 (wlan0) Interface Status	38
Network 2 (wlan0) Interface Configuration	38
Network 2 (wlan0) WLAN Link Status	40
Network 2 (wlan0) WLAN Link Configuration	41
Network 2 (wlan0) WLAN Link Scan	42
WLAN Profiles	43
WLAN Profile	44
<b>6: Line, Tunnel, Terminal, and Host Settings</b>	<b>53</b>
Line 1 and Line 2 Settings	53
Line 1 Statistics	53
Line 1 Configuration	54
Line 1 Command Mode	55
Tunnel 1 and Tunnel 2 Settings	57
Tunnel 1 – Statistics	57
Accept Mode	58
Packing Mode	61
Serial Settings	62
Connect Mode	63
Modem Emulation	66
Start and Stop Characters	68
Disconnect Mode	68
AES Keys	69
Terminal Settings	71
Line Terminal Configuration	71
Network Terminal Configuration	72
Host Configuration	73
<b>7: Configuration Pin Manager</b>	<b>75</b>
Configurable Pin Manager	75
CPM: Configurable Pins	75
CPM: Groups	78
<b>8: Services Settings</b>	<b>81</b>

DNS Configuration	81
PPP Configuration	81
SNMP Configuration	83
FTP Configuration	84
TFTP Configuration	85
Syslog Configuration	85
HTTP Configuration	86
HTTP Statistics	87
HTTP Configuration	87
HTTP Authentication	89
RSS Settings	91
LPD Settings	92
LPD Configuration Page	93
<b>9: Security Settings</b>	<b>94</b>
SSH Settings	94
SSH Server's Host Keys	94
SSH Server's Authorized Users	95
SSH Client Known Hosts	97
SSH Client User Configuration	98
SSL Settings	100
<b>10: Maintenance and Diagnostics Settings</b>	<b>104</b>
Filesystem Configuration	104
Filesystem Statistics	104
Filesystem Browser	105
Protocol Stack Configuration	108
IP Address Filter	109
Query Port	110
Diagnostics	111
Hardware	111
MIB-II Statistics	112
IP Sockets	113
Ping	114
Traceroute	115
DNS Lookup	116
Memory	117
Buffer Pools	118
Processes	119
CPU Power Management	121

System Configuration _____	121
<b>11: Advanced Settings</b>	<b>123</b>
Email Configuration _____	123
Email Statistics _____	123
Email Configuration _____	124
Command Line Interface Settings _____	125
Command Line Interface Statistics _____	125
CLI Configuration _____	126
XML Configuration _____	128
XML: Export Configuration _____	128
XML: Export Status _____	130
XML: Import System Configuration Page _____	132
<b>12: Point-to-Point Protocol (PPP)</b>	<b>138</b>
<b>13: Tunneling</b>	<b>139</b>
Connect Mode _____	139
Accept Mode _____	140
Disconnect Mode _____	141
Packing Mode _____	141
Modem Emulation _____	142
Command Mode _____	142
Serial Line Settings _____	144
Statistics _____	144
<b>14: Security in Detail</b>	<b>145</b>
Secure Shell: SSH _____	145
SSH Server Configuration _____	145
SSH Client Configuration _____	146
Secure Sockets Layer (SSL) _____	147
Utilities _____	149
<b>15: Branding the MatchPort b/g Pro</b>	<b>150</b>
Web Manager Customization _____	150
Command Mode _____	150
<b>16: Updating Firmware</b>	<b>151</b>
Obtaining Firmware _____	151
Loading New Firmware _____	151
<b>A: Technical Support</b>	<b>152</b>
<b>B: Binary to Hexadecimal Conversions</b>	<b>153</b>

Converting Binary to Hexadecimal .....	153
Conversion Table .....	153
Scientific Calculator .....	154

## C: Warranty

155

## Figures

Figure 2-1. Sample Hardware Address .....	15
Figure 2-2. Product Label .....	16
Figure 4-1. Web Manager Home Page .....	21
Figure 4-2. Components of the Web Manager Page .....	22
Figure 4-3. Web Manager Menu Structure (1 of 7) .....	26
Figure 4-4. Web Manager Menu Structure (2 of 7) .....	27
Figure 4-5. Web Manager Menu Structure (3 of 7) .....	28
Figure 4-6. Web Manager Menu Structure (4 of 7) .....	29
Figure 4-7. Web Manager Menu Structure (5 of 7) .....	30
Figure 4-8. Web Manager Menu Structure (6 of 7) .....	31
Figure 4-9. Web Manager Menu Structure (7 of 7) .....	32
Figure 4-10. Device Status .....	33
Figure 5-1. Network 1 (eth0) Interface Status .....	34
Figure 5-2. Network 1 (eth0) Interface Configuration .....	35
Figure 5-3. Network 1 Ethernet Link .....	37
Figure 5-4. Network 2 (wlan0) Interface Status .....	38
Figure 5-5. Network 2 (wlan0) Interface Configuration .....	39
Figure 5-6. Network 2 (wlan0) Link Status .....	41
Figure 5-7. Network 2 (wlan0) Link Configuration .....	42
Figure 5-8. Network 2 (wlan0) WLAN Link Scan .....	43
Figure 5-9. WLAN Profiles .....	44
Figure 5-10. WLAN Profile Page .....	45
Figure 5-11. WLAN Profile Advanced Configuration .....	46
Figure 5-12. WLAN Profile Security Configuration .....	47
Figure 5-13. WLAN Profile Security -- WEP Settings .....	48
Figure 5-14. WLAN Profile Security -- WPA with PSK Authentication .....	49
Figure 5-15. WLAN Profile Security -- WPA2/IEEE 802.11i with PSK Authentication .....	50
Figure 5-16. WLAN Profile Security -- WPA with IEEE 802.1X Authentication .....	50
Figure 5-17. WLAN Profile Security -- WPA2/IEEE 802.11i with IEEE 802.1X Authentication .....	50
Figure 6-1. Line 1 Statistics .....	53
Figure 6-2. Line 1 Configuration .....	54
Figure 6-3. Line 1 Command Mode .....	56
Figure 6-4. Tunnel 1 .....	58
Figure 6-5. Tunnel 1 Accept Mode .....	59
Figure 6-6. Tunnel 1 Packing Mode .....	61
Figure 6-7. Tunnel 1 Serial Settings .....	62
Figure 6-8. Tunnel 1 Connect Mode .....	64
Figure 6-9. Tunnel 1 Modem Emulation .....	67
Figure 6-10. Tunnel 1 Start/Stop Chars .....	68
Figure 6-11. Tunnel 1 Disconnect Mode .....	69
Figure 6-12. AES Keys .....	70
Figure 6-13. Terminal on Line 1 Configuration .....	71
Figure 6-14. Terminal on Network Configuration .....	72
Figure 6-15. Host Configuration .....	73
Figure 7-1. CPM: CPs .....	76

Figure 7-2. CPM: Groups .....	78
Figure 8-1. DNS Settings.....	81
Figure 8-2. PPP Settings.....	82
Figure 8-3. SNMP Configuration .....	83
Figure 8-4. FTP Configuration .....	84
Figure 8-5. TFTP Configuration.....	85
Figure 8-6. Syslog .....	86
Figure 8-7. HTTP Statistics .....	87
Figure 8-8. HTTP Configuration .....	88
Figure 8-9. HTTP Authentication.....	90
Figure 8-10. RSS.....	91
Figure 8-11. LDP Statistics.....	92
Figure 8-12. LPD Configuration.....	93
Figure 9-1. SSH Server: Host Keys.....	94
Figure 9-2. SSH Server: Authorized Users .....	96
Figure 9-3. SSH Client: Known Hosts .....	97
Figure 9-4. SSH Client: Users .....	99
Figure 9-5. SSL .....	101
Figure 10-1. Filesystem Statistics.....	104
Figure 10-2. Filesystem Browser.....	106
Figure 10-3. Protocol Stack .....	108
Figure 10-4. IP Address Filter Configuration .....	110
Figure 10-5. Query Port Configuration .....	111
Figure 10-6. Diagnostics: Hardware .....	112
Figure 10-7. MIB-II Network Statistics.....	113
Figure 10-8. IP Sockets .....	114
Figure 10-9. Diagnostics: Ping .....	115
Figure 10-10. Diagnostics: Traceroute .....	116
Figure 10-11. Diagnostics: DNS Lookup .....	117
Figure 10-12. Diagnostics: Memory .....	118
Figure 10-13. Diagnostics: Buffer Pools.....	119
Figure 10-14. Diagnostics: Processes.....	120
Figure 10-15. CPU Power Management .....	121
Figure 10-16. System .....	122
Figure 11-1. Email Statistics.....	123
Figure 11-2. Email Configuration.....	124
Figure 11-3. Command Line Interface Statistics .....	126
Figure 11-4. Command Line Interface Configuration .....	127
Figure 11-5. XML: Export Configuration.....	129
Figure 11-6. XML Status Record: Export System Status .....	131
Figure 11-7. XML: Import Configuration .....	132
Figure 11-8. XML: Import Configuration from External File.....	133
Figure 11-9. XML: Import from Filesystem .....	134
Figure 11-10. XML: Import Line(s) from Single Line Settings on the Filesystem.....	136



# 1: Using This Guide

## Purpose and Audience

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

**Note:** This guide occasionally refers to the MatchPort b/g Pro as just the MatchPort.

## Summary of Chapters

The remaining chapters in this guide include:

Chapter	Description
<a href="#">2: Introduction</a>	Main features of the product and the protocols it supports. Includes technical specifications.
<a href="#">3: Using DeviceInstaller</a>	Instructions for viewing the current configuration using DeviceInstaller.
<a href="#">4: Configuration Using Web Manager</a>	Instructions for accessing Web Manager and using it to configure settings for the MatchPort b/g Pro.
<a href="#">5: Network Settings</a>	Instructions for using the web interface to configure Ethernet and WLAN settings.
<a href="#">6: Line, Tunnel, Terminal, and Host Settings</a>	Instructions for using the web interface to configure line, tunnel, terminal, and host settings.
<a href="#">7: Configuration Pin Manager</a>	Information about the Configurable Pin Manager (CPM) and how to set the configurable pins to work with a device.
<a href="#">8: Services Settings</a>	Instructions for using the web interface to configure settings for DNS, SNMP, FTP, and other services.
<a href="#">9: Security Settings</a>	Instructions for using the web interface to configure SSH and SSL security settings.
<a href="#">10: Maintenance and Diagnostics Settings</a>	Instructions for using the web interface to maintain the MatchPort b/g Pro, view statistics, files, and logs, and diagnose problems.
<a href="#">11: Advanced Settings</a>	Instructions for using the web interface to configure email, CLI, and XML settings.
<a href="#">12: Point-to-Point Protocol (PPP)</a>	Description of PPP on the MatchPort b/g Pro.
<a href="#">13: Tunneling</a>	Information about tunneling features available on the serial lines.

Chapter	Description
<a href="#">14: Security in Detail</a>	Description and configuration of SSH and SSL security settings.
<a href="#">15: Branding the MatchPort b/g Pro</a>	Instructions for customizing the MatchPort b/g Pro.
<a href="#">16: Updating Firmware</a>	Instructions for obtaining the latest firmware and updating the MatchPort b/g Pro.
<a href="#">A: Technical Support</a>	Instructions for contacting Lantronix Technical Support.
<a href="#">B: Binary to Hexadecimal</a>	Instructions for converting binary values to hexadecimal.
<a href="#">C: Warranty</a>	Lantronix's warranty statement.

## Additional Documentation

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

Document	Description
<b>MatchPort b/g Pro Integration Guide</b>	Information about the MatchPort b/g Pro hardware, testing the MatchPort b/g Pro using the demonstration board, and integrating the MatchPort b/g Pro into your product.
<b>MatchPort b/g Pro Command Reference</b>	Instructions for accessing Command Mode (the command line interface) using a Telnet connection or through the serial port. Detailed information about the commands.
<b>MatchPort Demo Kit Quick Start</b>	Instructions for getting the MatchPort b/g Pro demonstration board up and running.
<b>DeviceInstaller Online Help</b>	Instructions for using the Lantronix Windows-based utility to locate the MatchPort b/g Pro and to view its current settings.
<b>Com Port Redirector Quick Start and Online Help</b>	Instructions for using the Lantronix Windows-based utility to create virtual com ports.
<b>Secure Com Port Redirector User Guide</b>	Instructions for using the Lantronix Windows-based utility to create secure virtual com ports.

## 2: Introduction

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.

### 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. Please contact your sales representative if you need larger memory sizes.
- ◆ 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 device server connects serial devices such as those listed below to Ethernet Wi-Fi 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 device server contains a full-featured TCP/IP stack. Supported protocols include:

- ◆ ARP, IP, UDP, TCP, ICMP, BOOTP, DHCP, Auto IP, Telnet, DNS, FTP, TFTP, HTTP(S), SSH, SSL/TLS, SNMP, SMTP, RSS, PPP and Syslog for network communications and management.
- ◆ TCP, UDP, TCP/AES, UDP/AES, Telnet, SSH and SSL/TLS for tunneling to the serial port.
- ◆ TFTP, FTP, and HTTP for firmware upgrades and uploading files.
- ◆ IEEE802.11bg, WPA, WPA2/IEEE802.11i, IEEE802.1X, Personal (PSK), Enterprise (EAP-TLS, EAP-TTLS, PEAP, LEAP) for wireless connectivity.

## Evolution OS™

MatchPort b/g Pro incorporates Lantronix's Evolution OS™. Key features of the Evolution OS™ include:

- ◆ Built-in Web server for configuration and troubleshooting from Web-based browsers
- ◆ CLI configurability
- ◆ [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 popular Internet-based standards, the MatchPort b/g Pro enables users to configure, manage, and troubleshoot efficiently through a simplified browser-based interface that is accessible anytime from anywhere. All configuration and troubleshooting options are launched from a well-organized, multi-page interface. Users can access all functionality via a Web browser, allowing them flexibility and remote access. As a result, users can enjoy the advantages of decreased downtime (based on the troubleshooting tools) and the ability to implement configuration changes easily (based on 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.

## **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 makes 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), a rapidly emerging technology 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**

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

By protecting the privacy of serial data transmitted across public networks, users can maintain their existing investment in serial technology, while taking advantage of the highest data-protection levels possible.

SSH and SSL can:

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

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

## 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 Ethernet 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 three 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 MatchPort b/g Pro using a Graphical User Interface (GUI) on a PC attached to a network. (See [3: Using DeviceInstaller](#).)

**Web Manager:** Through a web browser, configure the MatchPort b/g Pro's settings using the Lantronix Web Manager. (See [4: Configuration Using Web Manager](#).)

**Command Mode:** There are two methods to accessing Command Mode: 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 Command Reference Guide](#) 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. The XML is easily editable with a standard text or XML editor. (See the [MatchPort b/g Pro Command Reference Guide](#) 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

## Product Information Label

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

- ◆ Bar code
- ◆ Serial number
- ◆ Product ID (name)
- ◆ Part number
- ◆ Hardware address (MAC address)

**Figure 2-2. Product Label**





## 3: Using DeviceInstaller

This chapter covers the steps for locating a MatchPort b/g Pro unit and viewing its properties and device details.

**Note:** For instructions on using DeviceInstaller to configure the IP address and related settings or for more advanced features, see the Device Installer online Help.

The MatchPort's default configuration is as follows:

- ◆ Two default profiles:
  - Infrastructure Mode SSID: *Lantronix Initial Infra Network*
  - Ad hoc mode SSID: *Lantronix Initial Adhoc Network*
- Note:** Both of these profiles are enabled by default. Infrastructure Mode is the first choice, then AdHoc mode. You can set your AP to match an SSID of Lantronix Initial Infra Network or connect with another wireless card in Adhoc mode with an SSID of Lantronix Initial Adhoc Network.
- ◆ No encryption
- ◆ BOOTP, DHCP, and AutoIP enabled.

The computer on which DeviceInstaller will be installed needs to have access to a wireless card with the same settings. Set the IP address to 0.0.0.0.

**Note:** AutoIP generates a random IP address in the range 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 using DeviceInstaller.

Follow the instructions on the product CD to install and run DeviceInstaller.

1. Click **Start→Programs → Lantronix→DeviceInstaller→DeviceInstaller**.
2. Click the MatchPort folder. The list of Lantronix MatchPort b/g Pro devices available displays.
3. Expand the list of MatchPorts by clicking the + symbol next to the MatchPort b/g Pro icon. Select the MatchPort b/g Pro unit by clicking its IP address to view its configuration.

### Viewing the MatchPort b/g Pro's Current Configuration

1. In the right page, click the **Device Details** tab. The current MatchPort b/g Pro configuration displays:

**Note:** The settings are display only in this table unless otherwise noted.

Current Settings	Description
<b>Name</b>	Name identifying the MatchPort b/g Pro.
<b>Group</b>	Configurable field. Enter a <b>group</b> to categorize the MatchPort b/g Pro. Double-click the field, type in the value, and press <b>Enter</b> to complete. This group name is not visible on other PCs or laptops using DeviceInstaller.
<b>Comments</b>	Configurable field. Enter <b>comments</b> for the MatchPort b/g Pro. Double-click the field, type in the value, and press <b>Enter</b> to complete. This description or comment is local to this PC and is not visible on other PCs or laptops using DeviceInstaller.
<b>Device Family</b>	Displays the MatchPort b/g Pro's device family type as <b>MatchPort</b> .
<b>Type</b>	Displays the device type as <b>MatchPort b/g Pro</b> .
<b>ID</b>	Displays the MatchPort b/g Pro's ID embedded within the unit.
<b>Hardware Address</b>	Displays the MatchPort b/g Pro's hardware (MAC) address.
<b>Firmware Version</b>	Displays the firmware currently installed on the MatchPort b/g Pro.
<b>Extended Firmware Version</b>	Provides additional information on the firmware version.
<b>Online Status</b>	Displays the MatchPort b/g Pro's 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).
<b>Telnet Enabled</b>	Indicates whether Telnet is enabled on this MatchPort b/g Pro.
<b>Telnet Port</b>	Displays the MatchPort b/g Pro's port for Telnet sessions.
<b>Web Enabled</b>	Indicates whether Web Manager access is enabled on this MatchPort b/g Pro.
<b>Web Port</b>	Non-configurable field. Displays the MatchPort b/g Pro's port for Web Manager configuration.
<b>Maximum Baud Rate Supported</b>	Displays the MatchPort b/g Pro's maximum baud rate.
<b>Firmware Upgradeable</b>	Displays <b>True</b> , indicating the MatchPort b/g Pro's firmware is upgradeable as newer version become available.
<b>IP Address</b>	Displays the MatchPort b/g Pro's current IP address. To change the IP address, click the <b>Assign IP</b> button on the DeviceInstaller menu bar.

Current Settings	Description
<b>IP Address was Obtained</b>	<p>Displays <b>Dynamically</b> if the MatchPort b/g Pro automatically received an IP address (e.g., from DHCP). Displays <b>Statically</b> if the IP address was entered manually.</p> <p>If the IP address was assigned dynamically, 2-4 of the following fields display:</p> <p><b>Obtain via DHCP</b> with values of <b>True</b> or <b>False</b>.</p> <p><b>Obtain via BOOTP</b> with values of <b>True</b> or <b>False</b>.</p> <p><b>Obtain via RARP</b> with values of <b>True</b> or <b>False</b>.</p> <p><b>Obtain via AutoIP</b> with values of <b>True</b> or <b>False</b>.</p>
<b>Subnet Mask</b>	Displays the subnet mask specifying the network segment on which the MatchPort b/g Pro resides.
<b>Gateway</b>	Displays the IP address of the router of this network. There is no default.
<b>Number of Ports</b>	Displays the number of ports on this MatchPort b/g Pro.
<b>Supports Configurable Pins</b>	Displays <b>True</b> , indicating configurable pins are available on the MatchPort b/g Pro.
<b>Supports Email Triggers</b>	Displays <b>True</b> , indicating email triggers are available on the MatchPort b/g Pro.
<b>Telnet Enabled</b>	Indicates whether Telnet is enabled on this MatchPort b/g Pro.
<b>Telnet Port</b>	Displays the MatchPort b/g Pro's port for Telnet sessions.
<b>Web Enabled</b>	Indicates whether Web Manager access is enabled on this MatchPort b/g Pro.
<b>Web Port</b>	Non-configurable field. Displays the MatchPort b/g Pro's port for Web Manager configuration.
<b>Maximum Baud Rate Supported</b>	Displays the MatchPort b/g Pro's maximum baud rate.
<b>Firmware Upgradeable</b>	Displays <b>True</b> , indicating the MatchPort b/g Pro's firmware is upgradeable as newer version become available.

## 4: Configuration Using Web Manager

This chapter describes how to configure the MatchPort b/g Pro using Web Manager, Lantronix's 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.

### Accessing Web Manager Through a Web Browser

Log into the MatchPort b/g Pro using a standard Web browser.

**Note:** Alternatively, access the Web Manager by selecting the **Web Configuration** tab on the DeviceInstaller window.

#### To access Web Manager:

1. Open a standard web browser (such as Netscape Navigator 6.x and above, Internet Explorer 5.5. and above, Mozilla Suite, Mozilla Firefox, or Opera).
2. Enter the IP address of the MatchPort b/g Pro in the address bar.

**Note:** The IP address may have been assigned manually using DeviceInstaller or the serial port (see the MatchPort b/g Pro Quick Start) or automatically by DHCP.

3. Enter your user name and password.

**Note:** The factory-default user name is **admin** and the factory-default password is **PASS**.

The Web Manager home page displays.

**Note:** The MatchPort b/g Pro Status page (the home page) displays the common MatchPort b/g Pro configuration and product information.

Figure 4-1. Web Manager Home Page

MatchPort™ b/g Pro

LANTRONIX®  
EVOLUTION OS™

Status

Network

WLAN Profiles

Line

Tunnel

Terminal

Host

CPM

DNS

PPP

SNMP

FTP

TFTP

Syslog

HTTP

RSS

CLI

Email

LPD

SSH

SSL

XML

Filesystem

Protocol Stack

IP Address Filter

Query Port

Diagnostics

CPU Power Mgmt

System

Device Status

Product Information

Product Type:	Lantronix MatchPort b/g Pro
Firmware Version:	1.0.0.0R2
Build Date:	Mar 27 2008 (11:32:32)
Serial Number:	00000015
Uptime:	0 days 00:34:34
Permanent Config:	Saved

Network Settings

Interface:	wlan0
Link:	Established (qwerty)
MAC Address:	00:20:4a:80:8c:8f
Host:	
IP Address:	192.168.10.118 / 255.255.255.0 (DHCP)
Default Gateway:	192.168.10.1 (DHCP)
Domain:	int.lantronix.com (DHCP)
Primary DNS:	172.16.1.4 (DHCP)
Secondary DNS:	67.134.130.200 (DHCP)

Line Settings

Line 1:	RS232, 115200, N, 8, 1, None
Line 2:	RS232, 9600, N, 8, 1, None

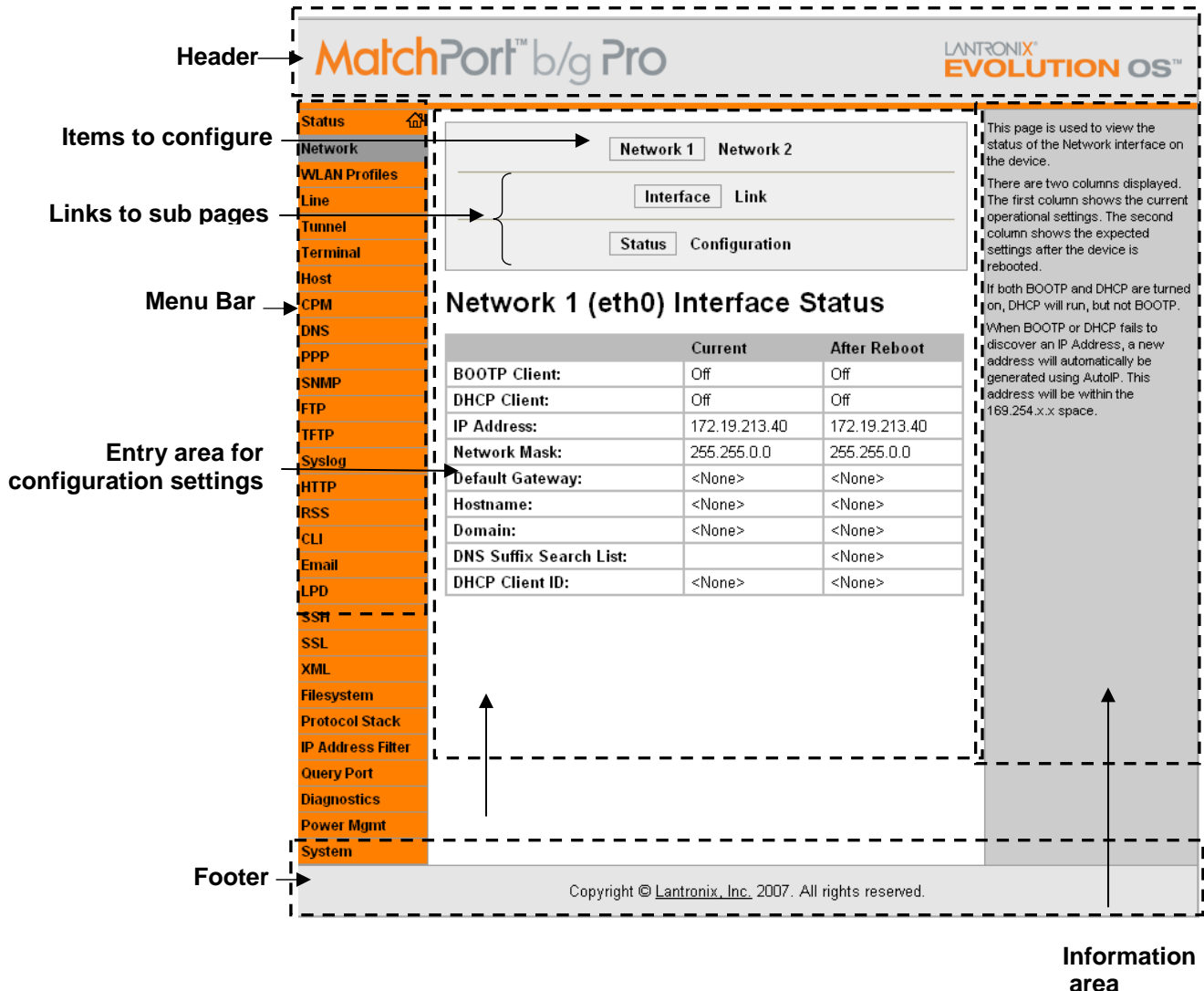
Tunneling	Connect Mode	Accept Mode
Tunnel 1:	Disabled	Waiting
Tunnel 2:	Disabled	Waiting

Copyright © Lantronix, Inc. 2007-2008. All rights reserved.

## Understanding the Web Manager Pages

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

Figure 4-2. Components of the Web Manager Page



- ◆ The header always displays at the top of the page. The header information remains the same regardless of the page displayed.
- ◆ The menu bar always displays at the left side of the page, regardless of the page displayed. The menu bar lists the names of the pages available in the Web Manager. To display a page, click it in the menu bar.
- ◆ The main area of the page has from one to three 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 section of many pages, you can select or enter new configuration settings. After you change settings, click the **Submit** button to apply the change. Some settings require you to reboot the MatchPort b/g Pro before the settings take effect. Those settings are identified in the appropriate sections in this chapter.

**Note:** Some pages display information such as statistics in this area rather than allow you to enter settings.

The bottom section of most pages shows the current configuration. In some cases you can take an action such as resetting.

- ◆ The information area shows information or instructions associated with the page.
- ◆ The footer displays at the bottom of the page. It contains copyright information and a link to the Lantronix home page.

## Navigating Through the Web Manager

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

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

Summary of Web Manager Pages

Page	Description	See Page
Status	Displays product information and network, line, and tunneling settings.	<a href="#">33</a>
Network	Displays status and lets you configure the network interfaces (Ethernet and WLAN on the MatchPort b/g Pro). The WLAN interface also lets you perform a scan of the wireless environment.	<a href="#">34</a>
WLAN Profiles	Lets you to view, create, delete, and modify a WLAN profile	<a href="#">42</a>
Line	Displays statistics and lets you change the current configuration and Command mode settings of two serial lines.	<a href="#">53</a>
Tunnel	Displays and lets you change the current configuration settings for up to two tunnels.	<a href="#">57</a>
Terminal	Displays and lets you change current settings for a terminal.	<a href="#">71</a>
Host	Displays and lets you change settings for a host on the network.	<a href="#">73</a>
CPM	Displays information about the Configurable Pins Manager (CPM) and how to set the configurable pins and pin groups to work with a device.	<a href="#">75</a>

Page	Description	See Page
DNS	Displays the current configuration of the DNS subsystem and lets you change primary and secondary DNS servers.	<a href="#">81</a>
PPP	Displays and lets you configure a network link using Point-to-Point Protocol (PPP) over a serial line.	<a href="#">81</a>
SNMP	Displays and lets you change the current Simple Network Management Protocol (SNMP) configuration settings.	<a href="#">83</a>
FTP	Displays statistics and lets you change the current configuration for the File Transfer Protocol (FTP) server.	<a href="#">84</a>
TFTP	Displays statistics and lets you change the current configuration for the Trivial File Transfer Protocol (TFTP) server.	<a href="#">85</a>
Syslog	Lets you specify the severity of events to log and the server and ports to which the syslog should be sent.	<a href="#">85</a>
HTTP	Displays HyperText Transfer Protocol (HTTP) statistics and lets you change the current configuration and authentication settings.	<a href="#">86</a>
RSS	Displays and lets you change current Really Simple Syndication (RSS) settings.	<a href="#">91</a>
CLI	Displays Command Line Interface (CLI) statistics and lets you change the current CLI configuration settings.	<a href="#">125</a>
Email	Displays email statistics and lets you clear the email log, configure email settings, and send an email.	<a href="#">123</a>
LPD	Displays LPD (Line Printer Daemon) Queue statistics and lets you configure the LPD and print a test page.	<a href="#">92</a>
SSH	Displays and lets you change the configuration settings for SSH server host keys, SSH server authorized users, SSH client known hosts, and SSH client users.	<a href="#">94</a>
SSL	Lets you upload an existing certificate or create a new self-signed certificate.	<a href="#">100</a>
XML	Lets you export XML configuration and status records, and import XML configuration records.	<a href="#">128</a>
Filesystem	Displays filesystem statistics and lets you browse the filesystem to create a file or directory, upload files using HTTP, copy a file, move a file, or perform TFTP actions.	<a href="#">104</a>
Protocol Stack	Lets you perform lower level network stack-specific activities.	<a href="#">108</a>
IP Address Filter	Lets you specify all the IP addresses and subnets that are allowed to send data to this device.	<a href="#">109</a>
Query Port	Displays and lets you change configuration settings for the query port.	<a href="#">110</a>
Diagnostics	Lets you perform various diagnostic procedures.	<a href="#">111</a>
CPU Power Mgmt	Lets you enable or disable CPU power management, its on-chip peripherals, and external memory.	<a href="#">121</a>
System	Lets you reboot the MatchPort b/g Pro, restore factory defaults, upload new firmware, change the MatchPort	<a href="#">121</a>

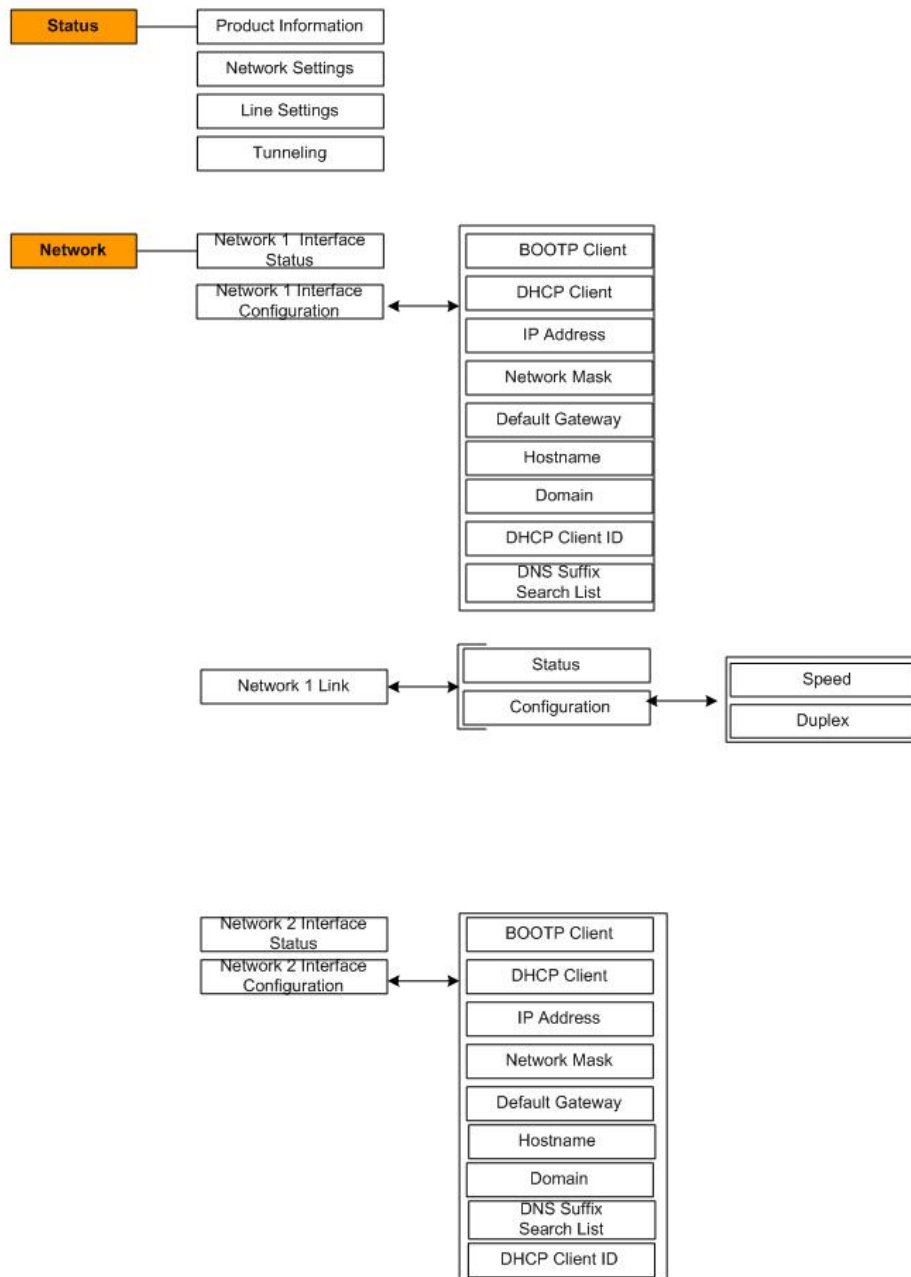


Page	Description	See Page
	b/g Pro's long and short names, and change the time setting.	

---

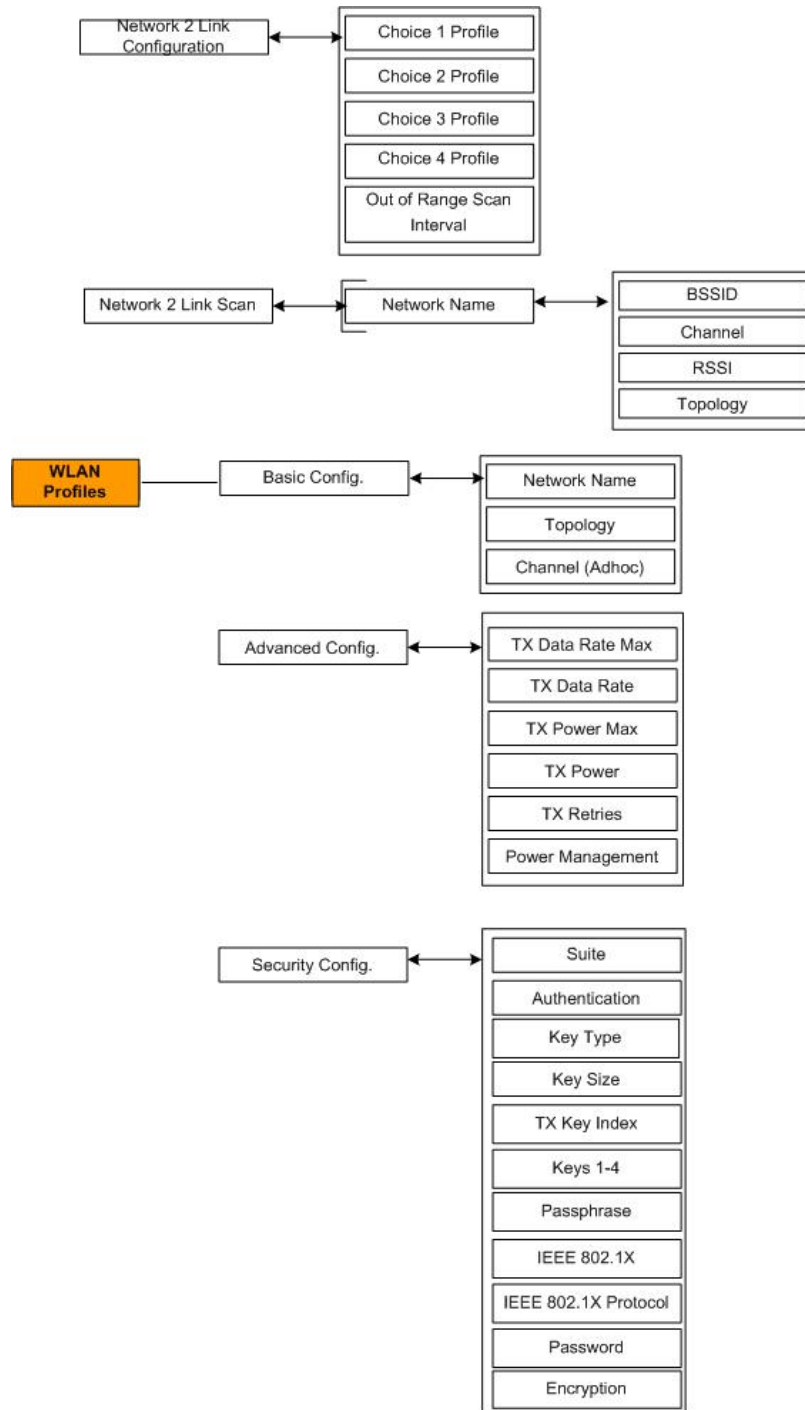
The following figures show the structure of the multilevel Web Manager configuration pages.

Figure 4-3. Web Manager Menu Structure (1 of 7)



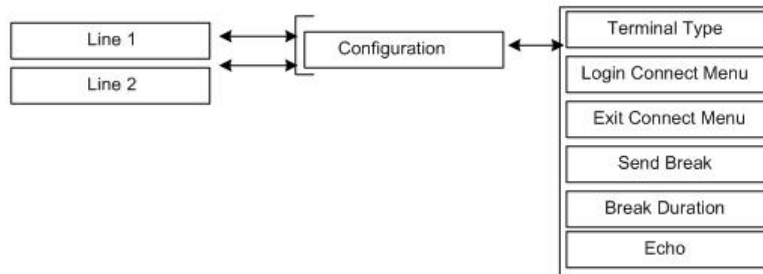
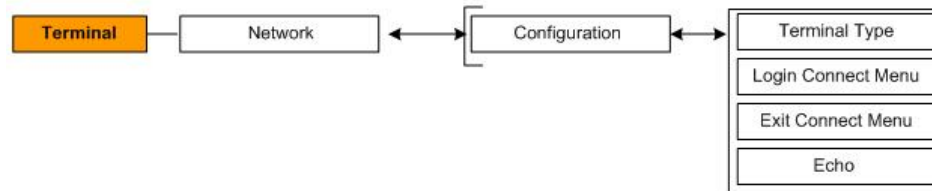
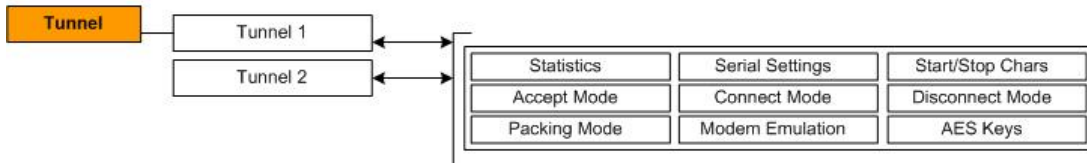
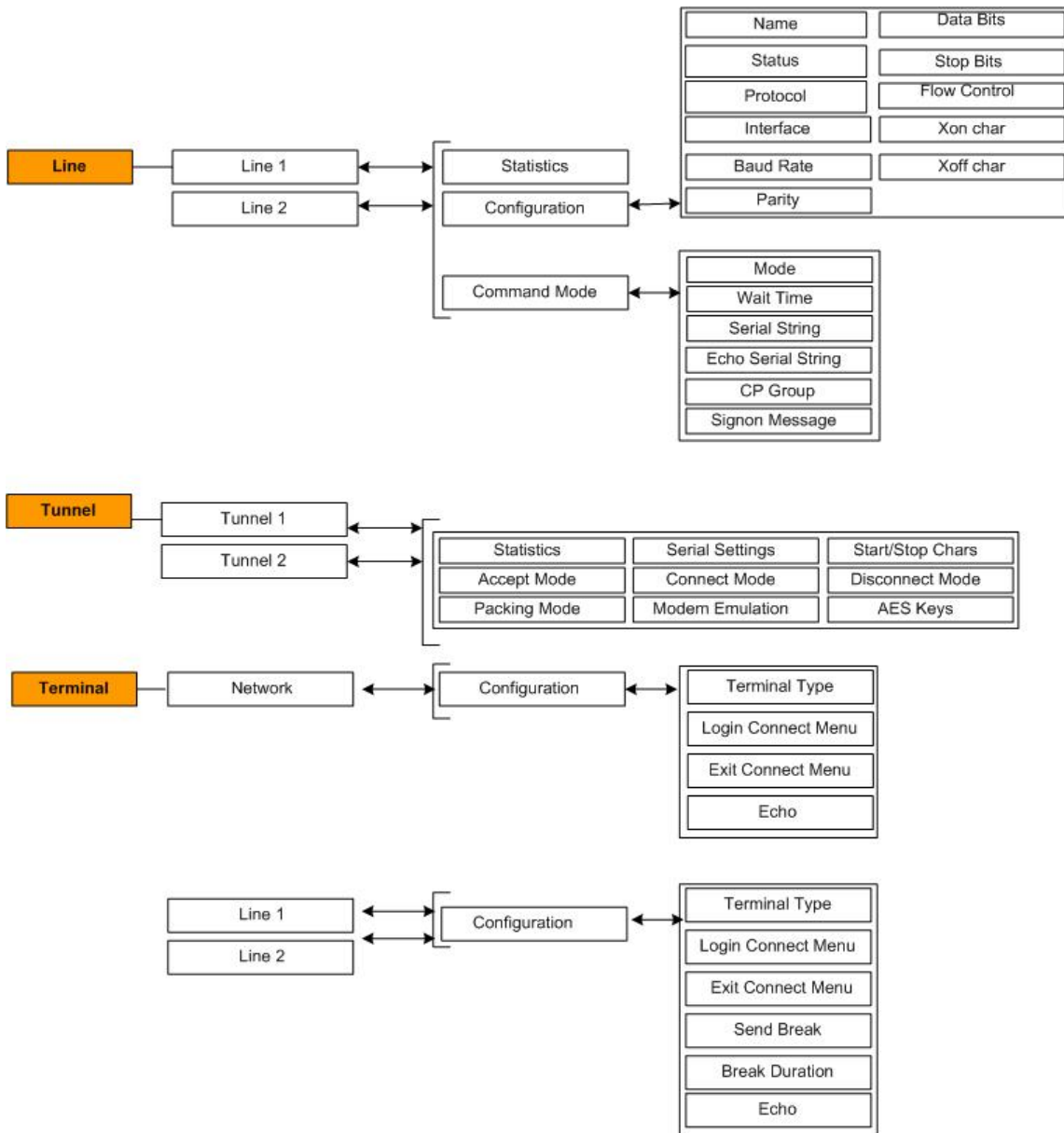
(continued on next page)

Figure 4-4. Web Manager Menu Structure (2 of 7)



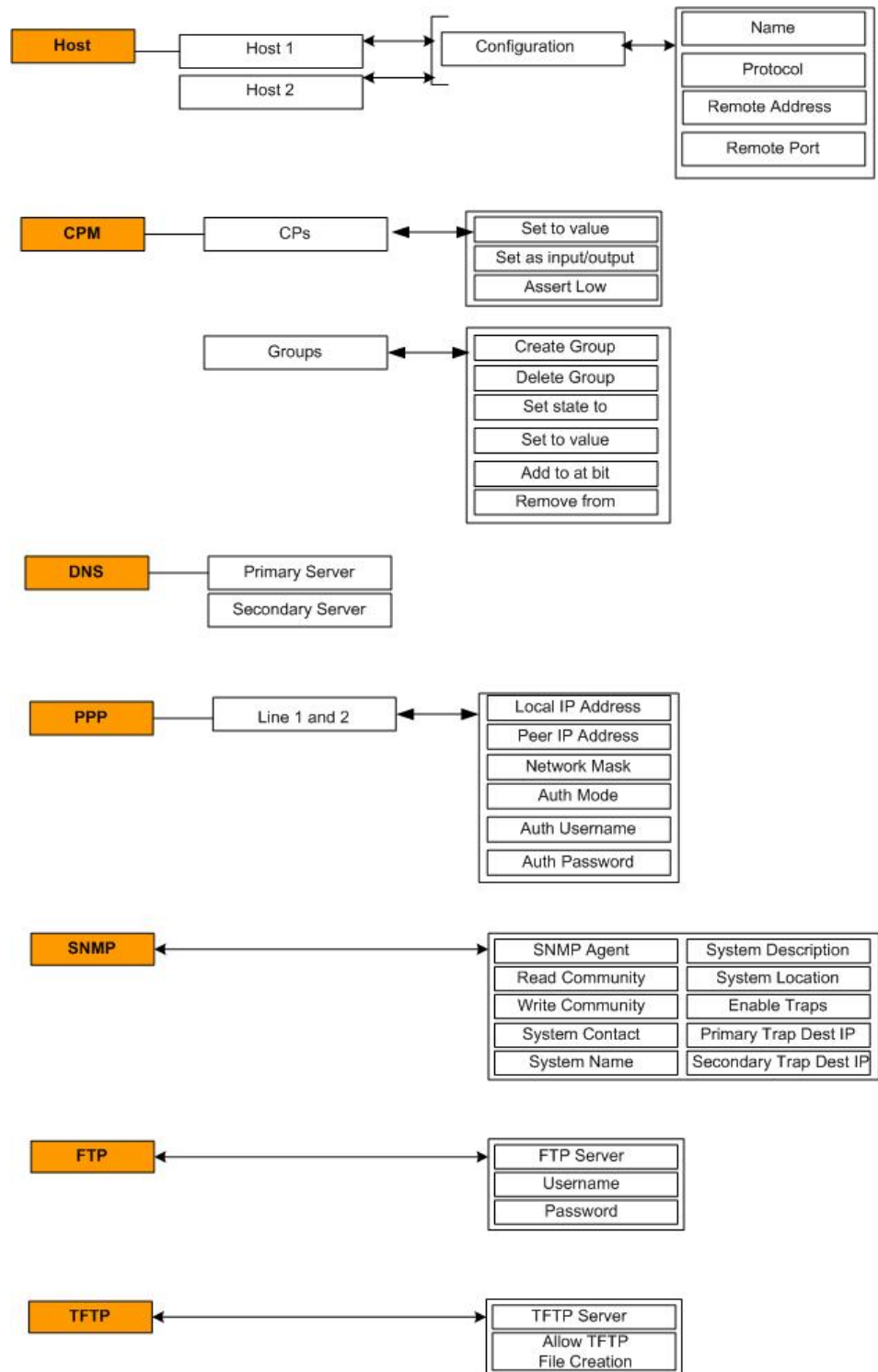
(continued on next page)

Figure 4-5. Web Manager Menu Structure (3 of 7)



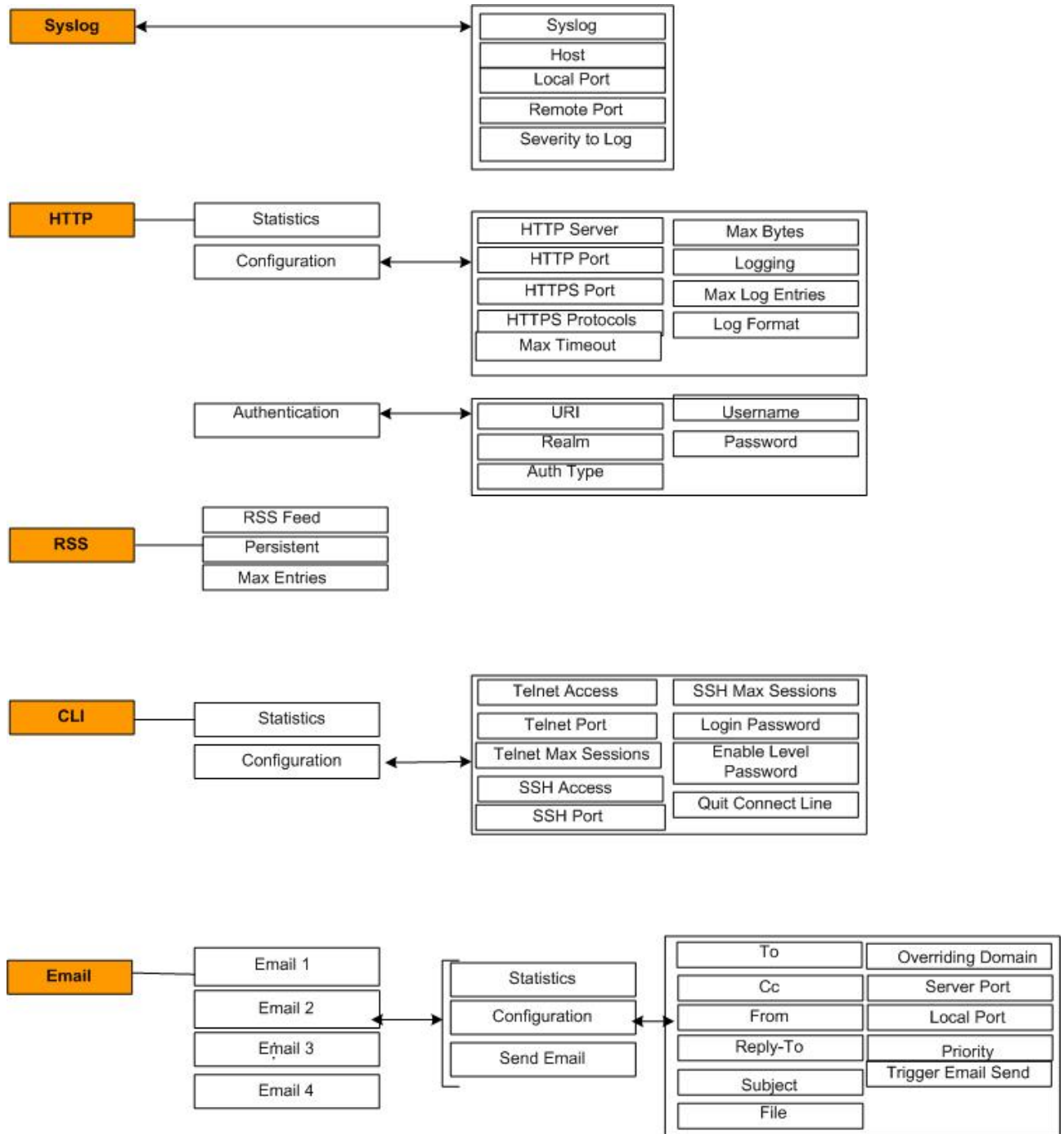
(continued on next page)

Figure 4-6. Web Manager Menu Structure (4 of 7)



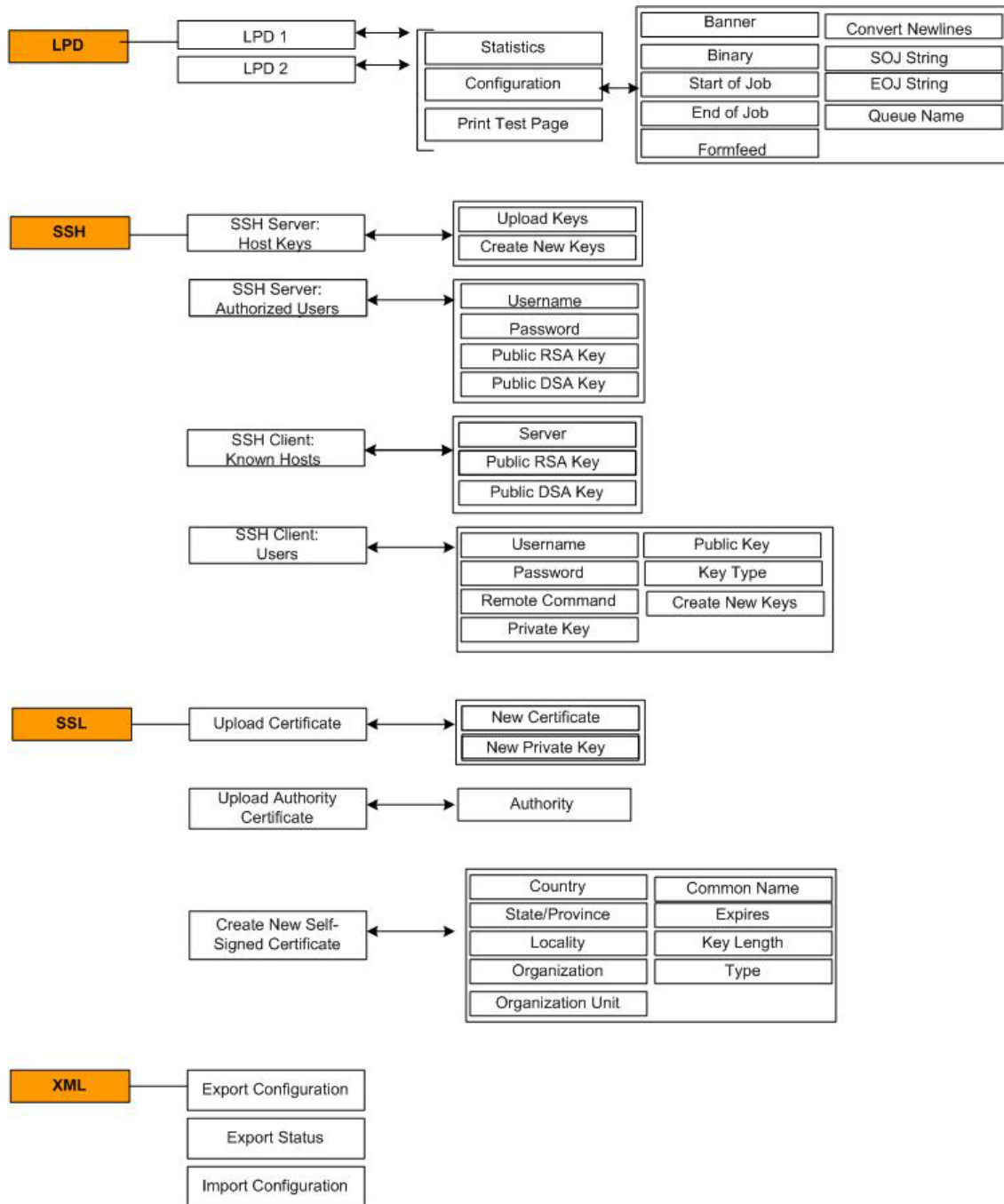
(continued on next page)

Figure 4-7. Web Manager Menu Structure (5 of 7)



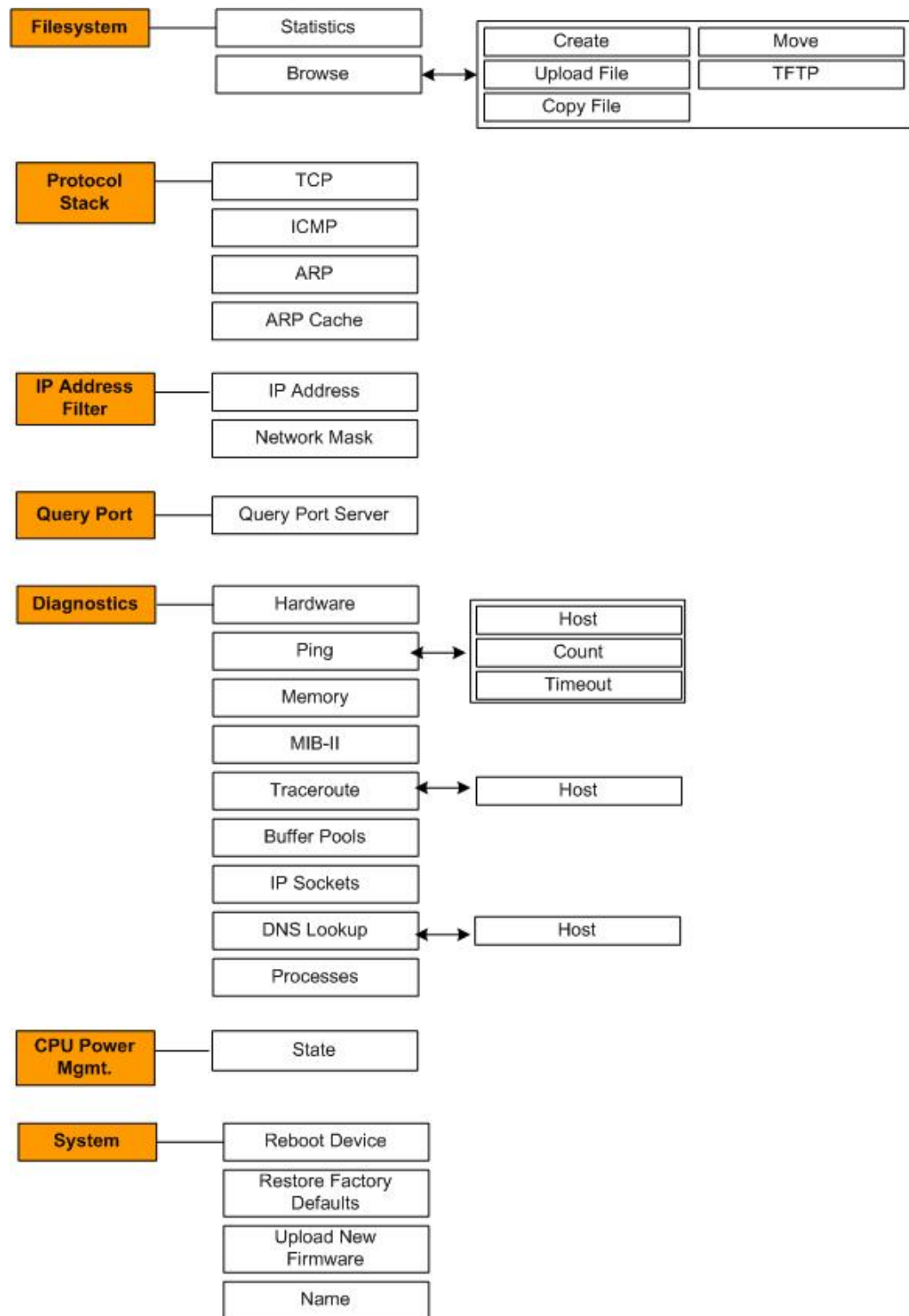
(continued on next page)

Figure 4-8. Web Manager Menu Structure (6 of 7)



(continued on the next page)

Figure 4-9. Web Manager Menu Structure (7 of 7)





## Device Status Page

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

Figure 4-10. Device Status

Device Status

Product Information		
Product Type:	Lantronix MatchPort b/g Pro	
Firmware Version:	9.9.9.9T9	
Build Date:	Dec 19 2007 (15:33:17)	
Serial Number:		
Uptime:	1 days 00:00:28	
Permanent Config:	Saved	
Network Settings		
Ethernet:	Auto 10/100 Mbps Auto Half/Full (100 Mbps Full)	
MAC Address:	00:20:4a:80:8c:a0	
Host:		
IP Address:	172.19.213.40 / 255.255.0.0	
Default Gateway:		
Domain:		
Primary DNS:		
Secondary DNS:		
Line Settings		
Line 1:	RS232, 9600, N, 8, 1, None	
Line 2:	RS232, 9600, N, 8, 1, None	
Tunneling	Connect Mode	Accept Mode
Tunnel 1:	Disabled	Waiting
Tunnel 2:	Disabled	Waiting

## 5: Network Settings

The Network Settings pages display the status of Ethernet (Network 1) and WLAN (Network 2) links and let you configure them on the device.

### Network Settings

#### 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 and then **Network 1, Interface**, and **Status** at the top of the page. The Network 1 (eth0) Interface Status page displays.

Figure 5-1. Network 1 (eth0) Interface Status

Network 1
Network 2

Interface
Link

Status
Configuration

### Network 1 (eth0) Interface Status

	Current	After Reboot
BOOTP Client:	Off	Off
DHCP Client:	Off	Off
IP Address:	172.19.213.40	172.19.213.40
Network Mask:	255.255.0.0	255.255.0.0
Default Gateway:	<None>	<None>
Hostname:	<None>	<None>
Domain:	<None>	<None>
DNS Suffix Search List:		<None>
DHCP Client ID:	<None>	<None>

This page is used to view the status of the Network interface on the device.

There are two columns displayed. The first column shows the current operational settings. The second column shows the expected settings after the device is rebooted.

If both BOOTP and DHCP are turned on, DHCP will run, but not BOOTP.

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

## 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 1** and **Interface Configuration** at the top of the page. The Network 1 (eth0) Interface Configuration page displays.

Figure 5-2. Network 1 (eth0) Interface Configuration

Network 1
Network 2

Interface
Link

Status
Configuration

### 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:	<input type="text" value="172.19.213.40/16"/>
Default Gateway:	<input type="text" value="&lt;None&gt;"/>
Hostname:	<input type="text"/>
Domain:	<input type="text"/>
DHCP Client ID:	<input type="text"/>
	<input checked="" type="radio"/> Text <input type="radio"/> Binary
Primary DNS:	<input type="text" value="&lt;None&gt;"/>
Secondary DNS:	<input type="text" value="&lt;None&gt;"/>

This page is used to configure the Network interface on the device. To see the effect of these items after a reboot, view the **Status** page.

The following items require a reboot to take effect:

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

If BOOTP or DHCP is turned on, any configured IP Address, Network Mask, Gateway, Hostname, or Domain will be ignored. BOOTP/DHCP will auto-discover and eclipse those configuration items.

If both BOOTP and DHCP are turned on, DHCP will run, but not BOOTP.

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

**IP Address** may be entered alone, in CIDR form, or with an explicit mask:  
 192.168.1.1 (default mask)  
 192.168.1.1/24 (CIDR)  
 192.168.1.1 255.255.255.0 (explicit mask)

**Hostname** must begin with a letter, continue with letter, number, or hyphen, and must end with a letter or number.

2. Enter or modify the following settings:

Network 1 Interface Configuration Page Settings	Description
State	State of the network link.
	<b>Enabled</b> = the interface is enabled.
	<b>Disabled</b> = the interface is disabled.

Network 1 Interface Configuration Page Settings	Description
<b>BOOTP Client</b>	<p>Select <b>On</b> or <b>Off</b>. At boot up the MatchPort b/g Pro will attempt to obtain an IP address from a BOOTP server.</p> <p><b>Notes:</b>  <i>Overrides the configured IP address, network mask, gateway, hostname, and domain.</i>  <i>When DHCP is <b>On</b>, the system automatically uses DHCP, regardless of whether BOOTP Client is <b>On</b>.</i></p>
<b>DHCP Client</b>	<p>Select <b>On</b> or <b>Off</b>. At boot up the MatchPort b/g Pro will attempt to lease an IP address from a DHCP server and maintain the lease at regular intervals.</p> <p><b>Note:</b> <i>Overrides BOOTP, the configured IP address, network mask, gateway, hostname, and domain.</i></p>
<b>IP Address</b>	<p>Enter the MatchPort b/g Pro's static IP address. 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 <b>Off</b>. Changing this value requires you to reboot the MatchPort b/g Pro.</p> <p><b>Note:</b> <i>When DHCP is enabled, the MatchPort b/g Pro tries to obtain an IP address from DHCP. If it cannot, the MatchPort b/g Pro uses an Auto IP address in the range of 169.254.xxx.xxx.</i></p>
<b>Default Gateway</b>	Enter the IP address of the router for this network. Clear the field (displays as <b>&lt;None&gt;</b> ). This address is only used for static IP address configuration.
<b>Hostname</b>	Enter the MatchPort b/g Pro's hostname. It must begin with a letter, continue with a sequence of letters, numbers, and/or hyphens, and end with a letter or number.
<b>Domain</b>	Enter the MatchPort b/g Pro's domain name.
<b>DHCP Client ID</b>	Enter the ID if the DHCP server uses a DHCP ID. The DHCP server's lease table displays IP addresses and MAC addresses for devices. The lease table displays the Client ID, in hexadecimal notation, instead of the MatchPort b/g Pro's MAC address.
<b>Primary DNS</b>	IP address of the primary name server. This entry is required if you choose to configure DNS (Domain Name Server) servers.
<b>Secondary DNS</b>	IP address of the secondary name server.

3. To save changes, click **Submit**. Some changes are applied immediately to the MatchPort b/g Pro. Changes to the following settings require a reboot for the changes to take effect:

- ◆ DHCP Client On/Off
- ◆ BOOTP Client On/Of
- ◆ IP address
- ◆ Network mask

- ◆ DHCP Client ID.

**Note:** If DHCP or BOOTP fails, AutoIP intervenes and assigns an address. In this case, the static IP (if configured) 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. The Network 1 (eth0) Ethernet Link page displays. From another Network page, click **Network 1** and **Link** at the top of the page.

Figure 5-3. Network 1 Ethernet Link

This page shows status and configuration of an Ethernet Link on the device.

The **Status** table shows the current negotiated settings.

The **Configuration** table shows the current range of allowed settings. After changing a setting, press **Submit** to make the changes on the device.

Network 1 (eth0) Ethernet Link	
<b>Status</b>	
Speed:	100 Mbps
Duplex:	Full
<b>Configuration</b>	
Speed:	<input checked="" type="radio"/> Auto <input type="radio"/> 10Mbps <input type="radio"/> 100Mbps
Duplex:	<input checked="" type="radio"/> Auto <input type="radio"/> Half <input type="radio"/> Full

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:

### Network 1-Ethernet Link Page Settings

### Description

#### Ethernet Link Speed

Select the Ethernet link speed. (Default is **Auto**.)

#### Ethernet Link Duplex

Select duplex mode. (Default is **Auto**.)

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

## WLAN Settings

### Network 2 (wlan0) Interface Status

This page shows the status of a WLAN link on the device.

To view the network interface status:

1. Click **Network** on the menu and then **Network 2, Interface**, and **Status** at the top of the page. The Network 2 (wlan0) Interface Status page displays.

Figure 5-4. Network 2 (wlan0) Interface Status

This page is used to view the status of the Network interface on the device.

There are two columns displayed. The first column shows the current operational settings. The second column shows the expected settings after the device is rebooted.

If both BOOTP and DHCP are turned on, DHCP will run, but not BOOTP.

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

	Current	After Reboot
BOOTP Client:	Off	Off
DHCP Client:	Off	On
IP Address:	<None>	<DHCP>
Network Mask:	<None>	<DHCP>
Default Gateway:	<None>	<DHCP>
Hostname:	<None>	<DHCP>
Domain:	<None>	<DHCP>
DNS Suffix Search List:		<DHCP>
DHCP Client ID:	<None>	<None>

There are two columns on the page. The first shows the current operational settings. The second shows the expected settings after the reboot.

If both BOOTP and DHCP are turned on, DHCP will run, but BOOTP will not. When BOOTP or DHCP fails to discover an IP address, AutoIP automatically generates a new address. This address will be within the 169.254.x.x space.

### Network 2 (wlan0) Interface Configuration

This page lets you configure the network interface on the device. To see the effect of these items after a reboot, view the Status page.

To view the Network 2 interface:

1. Click **Network** on the menu and then **Network 2, Interface**, and **Configuration** on the top of the page. The Network 2 (wlan0) Interface Configuration page displays.

Figure 5-5. Network 2 (wlan0) Interface Configuration

Network 1
**Network 2**

---

Interface
Link

---

Status
**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:	<input type="text" value="&lt;None&gt;"/>
Default Gateway:	<input type="text" value="&lt;None&gt;"/>
Hostname:	<input type="text"/>
Domain:	<input type="text"/>
DHCP Client ID:	<input type="text"/>
	<input checked="" type="radio"/> Text <input type="radio"/> Binary
Primary DNS:	<input type="text" value="&lt;None&gt;"/>
Secondary DNS:	<input type="text" value="&lt;None&gt;"/>

This page is used to configure the Network interface on the device. To see the effect of these items after a reboot, view the **Status** page.

The following items require a reboot to take effect:

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

If BOOTP or DHCP is turned on, any configured IP Address, Network Mask, Gateway, Hostname, or Domain will be ignored. BOOTP/DHCP will auto-discover and eclipse those configuration items.

If both BOOTP and DHCP are turned on, DHCP will run, but not BOOTP.

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

**Hostname** must begin with a letter, continue with letter, number, or hyphen, and must end with a letter or number.

2. Enter or modify the following settings:

Network 2 Interface Configuration Page Settings	Description
<b>State</b>	State of the WLAN interface.  <b>Enabled</b> = the interface is enabled  <b>Disabled</b> = the interface is disabled
<b>BOOTP Client</b>	Select <b>On</b> or <b>Off</b> . Overrides the configured IP address, network mask, gateway, hostname, and domain. <i><b>Note:</b> When DHCP is <b>On</b>, the system automatically uses DHCP, regardless of whether BOOTP Client is <b>On</b>.</i>
<b>DHCP Client</b>	Select <b>On</b> or <b>Off</b> . Overrides the configured IP address, network mask, gateway, hostname, and domain.

Network 2 Interface Configuration Page Settings	Description
<b>IP Address</b>	<p>Enter the MatchPort b/g Pro's static IP address.</p> <p>The IP address consists of four octets separated by a period and is used if BOOTP and DHCP are both set to <b>Off</b>. Changing this value requires you to reboot the MatchPort b/g Pro.</p> <p><b>Note:</b> When DHCP is enabled, the MatchPort b/g Pro tries to obtain an IP address from DHCP. If it cannot, the MatchPort b/g Pro uses an Auto IP address in the range of 169.254.xxx.xxx.</p>
<b>Default Gateway</b>	<p>Enter the IP address of the router for this network. Blank the field to remove it (displays as <b>&lt;None&gt;</b>). This address is only necessary and will be used only for static IP address configuration.</p>
<b>Hostname</b>	<p>Enter the MatchPort b/g Pro's hostname. It must begin with a letter, continue with a letter, number, or hyphen, and end with a letter or number.</p>
<b>Domain</b>	<p>Enter the MatchPort b/g Pro's domain name.</p>
<b>DHCP Client ID</b>	<p>Enter the ID if the DHCP server uses a DHCP ID. The DHCP server's lease table displays IP addresses and MAC addresses for devices. The lease table displays the Client ID, in hexadecimal notation, instead of the MatchPort b/g Pro's MAC address.</p>
<b>Primary DNS</b>	<p>Enter the IP address of the primary name server. This entry is required if you choose to configure DNS (Domain Name Server) servers.</p>
<b>Secondary DNS</b>	<p>IP address of the secondary name server.</p>

- If you have made changes, click **Submit**.

## Network 2 (wlan0) WLAN Link Status

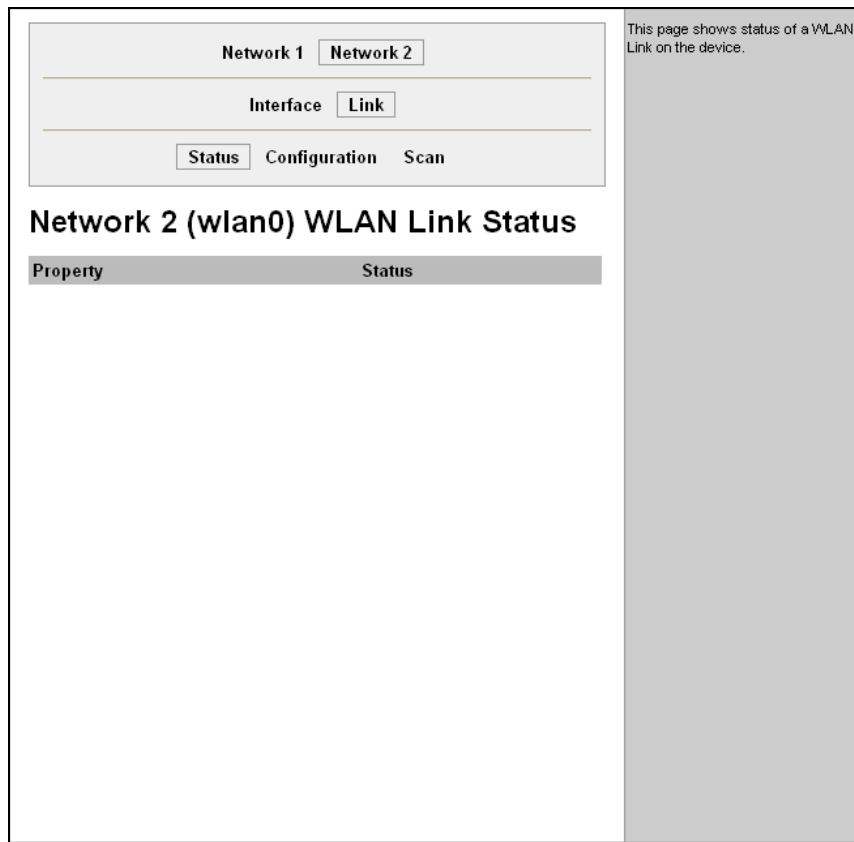
This page shows the status of a WLAN link on the device.

### To view the status of a WLAN link:

- Click **Network** on the menu and then **Network 2, Link**, and **Status** on the top of the page. The Network 2 (wlan0) Link Status page displays.



Figure 5-6. Network 2 (wlan0) Link Status



## Network 2 (wlan0) WLAN Link Configuration

This page lets you view and select configurations (profiles) in order of precedence.

### To view or select configurations:

1. Click **Network** on the menu and then **Network 2**, **Link**, and **Configuration** at the top of the page. The Network 2 (wlan) WLAN Link Configuration page displays.

Figure 5-7. Network 2 (wlan0) Link Configuration

Network 1

Network 2

Interface

Link

Status

Configuration

Scan

### 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

This page shows configuration of a WLAN Link on the device.

The configuration details are stored in one or more **WLAN Profile**. List the selected WLAN Profiles in order of preference here.

Use the **Apply** button to try out settings on the WLAN without saving them to Flash. If the settings do not work, when you reboot the device, it will still have the original settings.

Use the **Submit** button to both update the WLAN settings and save them to Flash.

The first time you log in, the two default configurations display as **Choice 1 Profile** and **Choice 2 Profile**. To delete a default configuration so you can replace it with your own, see [WLAN Profiles](#) on page 43.

- In the **Choice Profile** fields, enter the names of your profiles in order of preference. (To set up a profile, see page 35.)
- To save changes, click **Submit**. Changes are applied immediately.

### Network 2 (wlan0) WLAN Link Scan

This page shows a scan of the wireless devices within range of the MatchPort b/g Pro.

#### To scan wireless devices within range:

- Click **Network** on the menu and then **Network 2**, **Link**, and **Scan** at the top of the page. The Network 2 (wlan) WLAN Link Scan page displays.

Figure 5-8. Network 2 (wlan0) WLAN Link Scan

This page shows a scan of the wireless devices within range of the device. It reports: Network name (Service Set Identifier), Basic Service Set Identifier, Channel number, Received Signal Strength Indication, Topology (Infrastructure or Adhoc)

Network 1 **Network 2**

Interface **Link**

Status Configuration **Scan**

### Network 2 (wlan0) WLAN Link Scan

Network name:

Network name	BSSID	Ch	RSSI	T
<input type="button" value="Scan"/>				

2. Fill in the network name for a filtered response or leave it blank to see all networks
3. Click the **Scan** button. The following information displays about each wireless device within range:

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





## WLAN Profiles

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

**To open the WLAN Profiles page:**

1. On the menu, click **WLAN Profiles**. The WLAN Profiles page displays.

Figure 5-9. WLAN Profiles

WLAN Profiles	
<b>View or Edit:</b> <div>  default_adhoc_profile </div> <div>  default_infrastructure_profile </div>	<b>Delete:</b> <div>  </div> <div>  </div>
<b>Create new profile:</b> <input type="text"/>	

This page allows view, edit, deletion or creation of a WLAN Profile on the device.

Select a profile for editing by clicking the page icon; this takes you to the Basic Configuration web page.

Delete a profile by clicking the red X icon.

Create a new profile by entering a name in the text box, then click the Select button which will appear. The new profile is initially saved with default parameter values.

2. **To create a profile:**

- a) Enter a name for the profile in the **Create new profile** field and click **Submit**. A page icon and the profile name display above.
- b) Click the icon. The WLAN Profile page displays.
- c) Continue to WLAN Profile in this section.
- d) Click the icon beside the profile in the list above. The WLAN Profile page displays.
- e) Continue to WLAN Profile in this section.

3. **To delete a profile**, click the **X** to the right of the profile.

## WLAN Profile

This page allows you to configure basic, advanced, and security settings for a WLAN profile.

If you make any changes to the profile configuration, you have two options:

- ◆ To try out the settings without saving them, click **Apply**.
- ◆ To apply and save changes to permanent memory immediately, click **Submit**.

Figure 5-10. WLAN Profile Page

## WLAN Profile "newprofile"

Basic Configuration	
Network Name:	<input type="text"/>
Topology:	<input type="radio"/> Infrastructure <input checked="" type="radio"/> Adhoc
Channel:	<input type="text" value="1"/>
Advanced Configuration	
TX Data Rate Maximum:	54 Mbps <input type="button" value="v"/>
TX Data Rate:	<input type="radio"/> Fixed <input checked="" type="radio"/> Auto-reduction
TX Power Maximum:	<input type="text" value="14"/> dBm
TX Power:	<input checked="" type="radio"/> Fixed <input type="radio"/> Adaptation
TX Retries:	<input type="text" value="4"/>
Power Management:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Security Configuration	
Suite:	None <input type="button" value="v"/>

This page shows configuration of a WLAN Profile on the device.

In the **Basic Configuration** section, choice of **Topology** affects the makeup of configurables in that section and in the **Advanced Configuration** section.

In the **Advanced Configuration** section, if **Power Management** is enabled, specify the **Power Management Interval**.

In the **Security Configuration** section, choice of **Suite**, **Key Type**, **Authentication**, and **IEEE 802.1X** (when visible) affect the makeup of other configurables in that section.

Use the **Apply** button to try out settings on the WLAN without saving them to Flash. If the settings do not work, when you reboot the device, it will still have the original settings.

Use the **Submit** button to both update the WLAN settings and save them to Flash.

### Basic Configuration

WLAN Profile Page Basic Settings	Description
<b>Network Name</b>	Enter the name of the wireless network (SSID).
<b>Topology</b>	<p>Select <b>Infrastructure</b> (ESS) mode or <b>Adhoc</b> (IBSS) mode.</p> <p><b>Infrastructure:</b> mode that communicates with access points.</p> <p><b>Adhoc:</b> mode that communicates only with other clients.</p> <p><i>Note:</i> Your selection affects the settings displayed in this section and the Advanced section of this page.</p>
<b>Channel</b> (Displays for Adhoc mode)	Enter the radio channel for the Adhoc network.

## Advanced Configuration

Figure 5-11. WLAN Profile Advanced Configuration

Advanced Configuration	
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 checked="" type="radio"/> Fixed <input type="radio"/> Adaptation
TX Retries:	4
Power Management:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Power Management Interval:	1 beacons (100 ms each)

WLAN Advanced Security Settings	Description
TX Data Rate Maximum	Enter the maximum rate of data transmission. The default is <b>54 Mbps</b> .
TX Data Rate	<p>MatchPort b/g Pro lets you control the transmission data rate or controls it automatically.</p> <p><b>Fixed</b> = keeps the transmission rate at the configured maximum.</p> <p><b>Auto-reduction</b> = allows the MatchPort to reduce the data rate from the maximum automatically depending on link quality.</p>
TX Power Maximum	Maximum transmission output power in dBm.
TX Power	<p>Select the type of radio power control.</p> <p><b>Fixed</b> = keeps the transmission output power at the configured maximum.</p> <p><b>Adaptation</b> = 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.</p>
TX Retries	Number of times the MatchPort will attempt to transmit data before the packet is deemed lost.
Power Management	<p>Power management reduces the overall power consumption of the MatchPort unit, but can increase latency.</p> <p><b>Enabled</b> = allows the MatchPort to turn off the receiver when it is idling.</p> <p><b>Disabled</b> = keeps the receiver on at all times.</p>

WLAN Advanced Security Settings	Description
<b>Power Management Interval</b> (Displays if <b>Power Management</b> is enabled)	Number of beacons (100 ms) between 1 and 5. The above-mentioned latency increase can be up to this number x 100ms.

### Security Configuration

This section of the page is for configuring security settings for a WLAN Profile. The MatchPort b/g Pro features WEP, WPA, and WPA2/IEEE 802.11i to secure all wireless communication. 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.

Figure 5-12. WLAN Profile Security Configuration



**Note:** Depending on your choices for **Suite**, **Key Type**, **Authentication**, and **IEEE 802.1x**, different fields display.

WLAN Profile Security Settings (Adhoc or Infrastructure)	Description
<b>Suite</b>	<p>Select one of the following types of security. They are listed in ascending order of degree of security:</p> <p><b>None</b> = no authentication or encryption method will be used.</p> <p><b>WEP</b> = Wired Equivalent Privacy</p> <p><b>WPA</b> = WiFi Protected Access</p> <p><b>WPA2/IEEE 802.11i</b> = Robust Secure Network</p>

### 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 5-13. 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>

WLAN Profile Security Configuration WEP Settings	Description
Authentication	<p>Select an authentication scheme from the drop-down list.</p> <p><b>Shared</b> = encryption keys of both parties are compared as a form of authentication. If mismatched, no connection is established.</p> <p><b>Open</b> = 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.</p>
Key Type	<p>Select the format of the security key.</p> <p><b>Passphrase</b> = A text of up to 63 characters converted to 4 encryption keys.</p> <p><b>Hex</b> = 4 individually entered encryption keys consisting of hexadecimal digits.</p>
Key Size	<p>Key size in bits. Select <b>40</b> for WEP40 and WEP64, select <b>104</b> for WEP104 and WEP128.</p>
TX Key Index (Displays if <b>Key Type</b> is <b>Hex</b> )	<p>Select one of four indexes listing keys for transmitting data. Reception is allowed with all four keys.</p>



WLAN Profile Security Configuration WEP Settings	Description
<b>Keys 1-4</b> (Displays if <b>Key Type</b> is <b>Hex</b> )	Enter one or more encryption keys in hexadecimal format. Enter 10 hexadecimal digits (0-9, a-f) for WEP40 and 26 for WEP104. The already configured keys are not displayed for security reasons.
<b>Passphrase</b> (Displays if <b>Key Type</b> is <b>Passphrase</b> )	<p>The passphrase consists of text of up to 63 characters and is hashed into 4 encryption keys using the Neesus Datacom algorithm (for WEP64) or MD5 (for WEP128).</p> <p><b>Note:</b> Lantronix recommends using a passphrase of 20 characters or more for maximum security. Spaces and punctuation characters are permitted.</p> <p><b>Note:</b> 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.</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 5-14. WLAN Profile Security – WPA with PSK Authentication

Security Configuration	
Suite:	WPA <input type="button" value="v"/>
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
<input type="button" value="Apply"/> <input type="button" value="Submit"/>	

Figure 5-15. 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

Figure 5-16. 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

Figure 5-17. 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

WLAN Profile Security WPA & WPA2 Settings	Description
<b>Authentication</b>	<p>Select an authentication scheme.</p> <p><b>PSK</b> = Pre-Shared Key. The same key needs to be entered on both sides of the connection. That is on the MatchPort b/g Pro and on the Access Point.</p> <p><b>IEEE 802.1X</b> = 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.</p>
<b>Key Type</b> (Displays if <b>Authentication</b> is <b>PSK</b> )	<p>Select the format of the security key.</p> <p><b>Passphrase</b></p> <p><b>Hex</b></p>
<b>Key</b> (Displays if <b>Key Type</b> is <b>Hex</b> )	<p>64 hexadecimal digits.</p>
<b>Passphrase</b> (Displays if <b>Key Type</b> is <b>Passphrase</b> )	<p>The passphrase consists of text of up to 63 characters and is hashed into a 32 bytes encryption key using a repeated SHA1 algorithm.</p> <p><i><b>Note:</b> Lantronix recommends using a passphrase of 20 characters or more for maximum security. Spaces and punctuation characters are permitted.</i></p> <p><i><b>Note:</b> 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.</i></p>
<b>IEEE 802.1X</b> (Displays if <b>Authentication</b> is <b>IEEE 802.1X</b> )	<p>From the drop-down list, select the protocol to use to authenticate the WLAN client.</p> <p><b>LEAP</b> = Lightweight Extensible Authentication Protocol.</p> <p>A derivative of the original <b>Cisco LEAP</b>, which was a predecessor of 802.1X. Real <b>Cisco LEAP</b> uses a special MAC layer authentication (called <b>Network EAP</b>) and cannot work with <b>WPA/WPA2</b>. 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.</p> <p><b>EAP-TLS</b> = Extensible Authentication Protocol - Transport Layer Security.</p> <p>Uses the latest incarnation of the <b>Secure Sockets Layer (SSL)</b> standard and is the most secure because it requires authentication certificates on both the network side and the MatchPort b/g Pro side.</p> <p><b>EAP-TTLS</b> = Extensible Authentication Protocol - Tunneled Transport Layer Security.</p> <p><b>PEAP</b> = Protected Extensible Authentication Protocol.</p> <p><b>EAP-TTLS</b> and <b>PEAP</b> 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 <b>EAP-TLS</b> to authenticate the server (network) side and establish an encrypted tunnel. This is called the outer-</p>

WLAN Profile Security WPA & WPA2 Settings	Description
	<p>authentication. Then a conventional authentication method (<b>MD5</b>, <b>MSCHAP</b>, etc.) is used through the tunnel to authenticate the MatchPort b/g Pro. This is called inner authentication.</p> <p><b>EAP-TTLS</b> and <b>PEAP</b> have been developed by different consortia and vary in details. Of which the most visible is the supported list of inner authentications.</p> <p><i>Note: When using <b>EAP-TLS</b>, <b>EAP-TTLS</b> or <b>PEAP</b> authority at least one authority certificate will have to be installed in the <b>SSL</b> configuration that is able to verify the Radius server's certificate. In case of <b>EAP-TLS</b> also a certificate and matching private key need to be configured to authenticate the MatchPort b/g Pro to the Radius server. For more information about <b>SSL</b> certificates see the Secure Sockets Layer (SSL) chapter.</i></p>
<b>EAP-TTLS Option</b> (Displays if <b>IEEE 802.1X</b> is <b>EAP-TTLS</b> )	<p>From the drop-down list, select the inner authentication.</p> <p><b>EAP-MSCHAPv2</b></p> <p><b>MSCHAPv2</b></p> <p><b>MSCHAP</b></p> <p><b>CHAP</b></p> <p><b>PAP</b></p> <p><b>EAP-MD5</b></p>
<b>PEAP Option</b> (Displays if <b>IEEE 802.X</b> is <b>PEAP</b> )	<p>From the drop-down list, select the inner authentication.</p> <p><b>EAP-MSCHAPv2</b></p> <p><b>EAP-MD5</b></p>
<b>Username</b> (Displays if <b>Authentication</b> is <b>IEEE 802.1X</b> )	<p>Userid for identifying the MatchPort b/g Pro to the Radius server in the network.</p>
<b>Password</b> (Displays if <b>Authentication</b> is <b>IEEE 802.1X</b> )	<p>Password for identifying the MatchPort b/g Pro to the Radius server in the network.</p>
<b>Encryption</b>	<p>Select one or more encryption types, listed from strongest to least strong. The selection will have to match the Access Points intended to connect with.</p> <p><b>CCMP</b> = Uses AES as basis and is the strongest encryption option.</p> <p><b>TKIP</b> = Uses WEP as the basis, but adds extra checks and variations for added protection.</p> <p><b>WEP</b> = Based on RC4.</p> <p><i>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.</i></p>

## 6: Line, Tunnel, Terminal, and Host Settings

### Line 1 and Line 2 Settings

The Line Settings pages display the status and statistics for each of the serial lines (ports). They also let you change the character format and Command Mode settings for the serial lines.

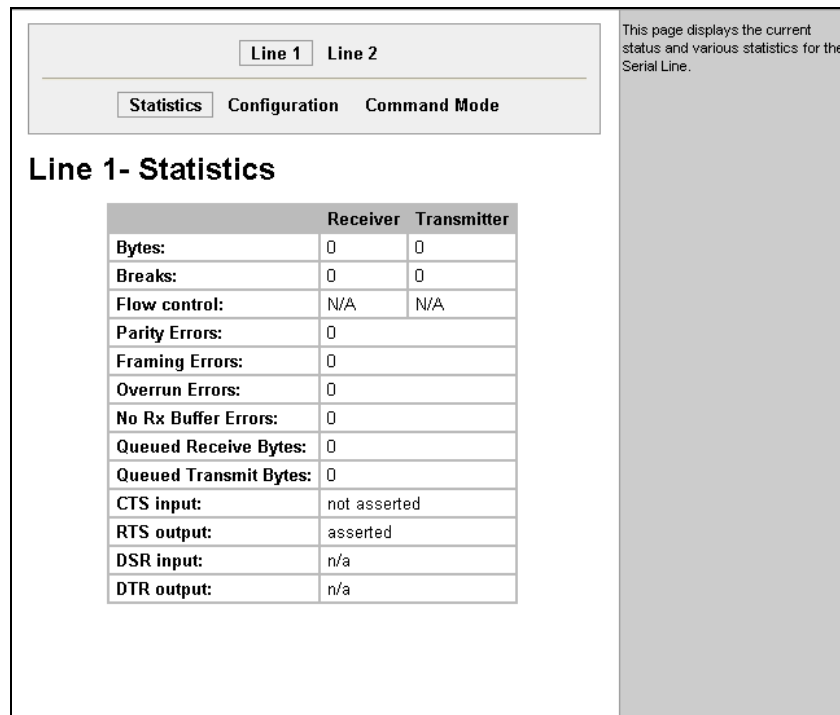
**Note:** The following section describes the steps to view and configure Line 1 settings; these steps also apply to Line 2 menu options.

#### Line 1 Statistics

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

1. Select **Line** on the menu bar. The Line 1 Statistics page displays.

Figure 6-1. Line 1 Statistics



This page displays the current status and various statistics for the Serial Line.

Line 1 Line 2

Statistics Configuration Command Mode

### 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:	n/a	
DTR output:	n/a	

## Line 1 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 Line 1:

1. Click **Line 1** and **Configuration** at the top of the page. The Line 1 Configuration page displays.

Figure 6-2. Line 1 Configuration

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

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

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

	Current Setting	Change Setting To
<b>Name:</b>		<input type="text"/>
<b>Status:</b>	Enabled	Enabled <input type="button" value="v"/>
<b>Protocol:</b>	Tunnel	Tunnel <input type="button" value="v"/>
<b>Interface:</b>	RS232	RS232 <input type="button" value="v"/>
<b>Baud Rate:</b>	115200	115200 <input type="button" value="v"/> Custom <input type="text"/>
<b>Parity:</b>	None	None <input type="button" value="v"/>
<b>Data Bits:</b>	8	8 <input type="button" value="v"/>
<b>Stop Bits:</b>	1	1 <input type="button" value="v"/>
<b>Flow Control:</b>	None	None <input type="button" value="v"/>
<b>Xon char:</b>	0x11 ( \17 )	<input type="text"/>
<b>Xoff char:</b>	0x13 ( \19 )	<input type="text"/>
		<input type="button" value="Submit"/>

2. Enter or modify the following settings:

Line - Configuration Page Settings	Description
<b>Name</b>	Enter a name for the line. The default <b>Name</b> is blank.
<b>Status</b>	Indicates whether the current line is enabled. To change the status, select <b>Enabled</b> or <b>Disabled</b> from the drop-down menu.
<b>Protocol</b>	Select the protocol for the line from the drop-down menu. The default is <b>None</b> .
<b>Interface</b>	Select the line's interface from the drop-down menu. The default is <b>RS232</b> .
<b>Baud Rate</b>	Select the MatchPort b/g Pro's baud rate from the drop-down menu. The default is <b>9600</b> .
<b>Parity</b>	Select the MatchPort b/g Pro's parity from the drop-down menu. The default is <b>None</b> .
<b>Data Bits</b>	Select the number of data bits from the drop-down menu. The default is <b>8</b> .

Line - Configuration Page Settings	Description
<b>Stop Bits</b>	Select the number of stop bits from the drop-down menu. The default is <b>1</b> .
<b>Flow Control</b>	Select the MatchPort b/g Pro's flow control from the drop-down menu. The default is <b>None</b> .
<b>Xon Char</b>	Specify the character to use to initiate a flow of data. When <b>Flow Control</b> is set to <b>Software</b> , specify <b>Xon char</b> . Prefix a decimal character with \ or a hexadecimal character with <b>0x</b> , or provide a single printable character. The default Xon char is <b>0x11</b> .
<b>Xoff Char</b>	When <b>Flow Control</b> is set to <b>Software</b> , specify <b>Xoff char</b> . Prefix a decimal character with \ or a hexadecimal character with <b>0x</b> , or provide a single printable character. The default Xoff char is <b>0x13</b> .

- Click **Submit**. Changes are applied immediately to the MatchPort b/g Pro.

## Line 1 Command Mode

Setting Command Mode enables the CLI on the serial line.

### To configure Line 1's Command Mode:

- Click **Line 1** and **Command Mode** at the top of the page. The Line 1 Command Mode page displays.

Figure 6-3. Line 1 Command Mode

Line 1
Line 2

Statistics
Configuration
Command Mode

### Line 1- Command Mode

**Mode:**

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

**Wait Time:**  milliseconds

**Serial String:**  ☒ Text ☐ Binary

**Echo Serial String:** ☐ Yes ☐ No

**CP Group:** Group:  Value:

**Signon Message:**  ☒ Text ☐ Binary

---

**Current Configuration**

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

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

The **Always** choice immediately enables Command Mode for the Serial Line.

The **Use Serial String** choice enables Command Mode when the Serial String is read on the Serial Line during boot time.

The **Use CP Group** choice 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.

The **Wait Time** specifies the amount of time to wait during boot time for the Serial String. This timer starts right after the Signon Message has been sent on the Serial Line.

The **Serial String** is a string of bytes that must be read on the Serial Line during boot time in order to enable Command Mode. It may contain a **time element** to specify a required delay in milliseconds x, formed as {x}.

The **Signon Message** is a string of bytes that is sent on the Serial Line during boot time.

**Binary** form is one or more byte values separated by commas. Each byte value may be decimal or Hexadecimal. Start Hexadecimal values with 0x.

2. Enter or modify the following settings:

Line - Command Mode Page Settings	Description
<b>Mode</b>	<p>Select the method of enabling Command Mode or choose to disable Command Mode.</p> <p><b>Always</b> = immediately enables Command Mode for the serial line.</p> <p><b>Use Serial String</b> = enables Command Mode when the serial string is read on the serial line during boot time.</p> <p><b>Use CP Group</b> = 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.</p> <p><b>Use both Serial String and CP Group</b> = the serial string and the value of the CP group must be matched to enable Command Mode.</p> <p><b>Disabled</b> = turns off Command Mode.</p>
<b>Wait Time</b>	Enter the wait time for the serial string during boot-up in milliseconds.
<b>Serial String</b>	Enter the serial string characters. Select a string type.



Line - Command Mode Page Settings	Description
	<p><b>Text</b> = string of bytes that must be read on the Serial Line during boot time to enable Command Mode. It may contain a <b>time element</b> in x milliseconds, in the format {x}, to specify a required delay.</p> <p><b>Binary</b> = string of characters representing byte values where each hexadecimal byte value starts with <b>0x</b> and each decimal byte value starts with <b>\</b>.</p>
<b>Echo Serial String</b>	Select <b>Yes</b> to enable echoing of the serial string at boot-up.
<b>CP Group</b>	Enter the name and decimal value of the CP group.
<b>Signon Message</b>	Enter the boot-up signon message. Select a string type.
	<p><b>Text</b> = string of bytes sent on the serial line during boot time.</p> <p><b>Binary</b> = one or more byte values separated by commas. Each byte value may be decimal or hexadecimal. Start hexadecimal values with <b>0x</b>.</p>

3. In the **Current Configuration** table, clear currently stored settings as necessary.
4. Click **Submit**. Changes are applied immediately to the MatchPort b/g Pro.

## Tunnel 1 and Tunnel 2 Settings

The Tunnel pages allow you to view current statistics and configure serial settings, Connect Mode, Accept Mode, Disconnect Mode, Packing Mode, start and stop characters, modem emulation, and AES keys.

**Note:** The following section describes the steps to view and configure Tunnel 1 settings; these steps also apply to Tunnel 2 menu options.

### Tunnel 1 – Statistics

1. Click **Tunnel** on the menu bar. The Statistics page for Tunnel 1 displays.

Figure 6-4. Tunnel 1

Tunnel 1
Tunnel 2

This page displays the current connection status and various statistics of the Tunnel.

Statistics

Accept Mode

Packing Mode

Serial Settings

Connect Mode

Modem Emulation

Start/Stop Chars

Disconnect Mode

AES Keys

### Tunnel 1- Statistics

Aggregate Counters	
Completed Connects:	0
Completed Accepts:	0
Disconnects:	0
Dropped Connects:	0
Dropped Accepts:	0
Octets forwarded from Serial:	0
Octets forwarded from Network:	0
Connect Connection Time:	0 days 00:00:00
Accept Connection Time:	0 days 00:00:00
Connect DNS Address Changes:	0
Connect DNS Address Invalids:	0

Connect Counters	
There is no active connection.	

Accept Counters	
There is no active connection.	

## Accept Mode

In Accept Mode, the MatchPort b/g Pro listens (waits) for incoming connections.

### To configure the tunnel's Accept Mode:

1. Click **Tunnel 1** and **Accept Mode** at the top of the page. The Tunnel 1 Accept Mode page displays.

Figure 6-5. Tunnel 1 Accept Mode

Tunnel 1
Tunnel 2

Statistics

**Accept Mode**

Packing Mode

Serial Settings

**Connect Mode**

Modem Emulation

Start/Stop Chars

**Disconnect Mode**

AES Keys

### Tunnel 1- Accept Mode

**Mode:**

☐ Disabled
 ☐ Enabled

☐ Any Character
 ☐ Modem Control Asserted

☐ Start Character
 ☐ Modem Emulation

**Local Port:**

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

**Flush Serial Data:** ☐ Enabled ☐ Disabled

**Block Serial Data:** ☐ On ☐ Off

**Block Network Data:** ☐ On ☐ Off

**TCP Keep Alive:**  seconds

**Email on Connect:**

**Email on Disconnect:**

**CP Set Group:**

**On Connection:**

**On Disconnection:**

**Password:**

**Prompt for Password:** ☐ On ☐ Off

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

**Disabled:** never started

**Enabled:** always started

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

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

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

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

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

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

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

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

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

The **CP Set Group** identifies a CP or CP Group whose value should change when a connection is established and dropped. **On Connection** specifies the value to set the CP or CP Group to when a connection is established and **On Disconnection** specifies the value that should be used when the connection is closed.

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

#### Current Configuration

Mode:	Enabled (Waiting)
Local Port:	10001
Protocol:	Tcp
Flush Serial Data:	Disabled
Block Serial Data:	Off
Block Network Data:	Off
TCP Keep Alives:	Default 45 seconds
Email on Connect:	<None>
Email on Disconnect:	<None>
CP Set Group:	<None>
On Connection Value:	0 (0x0)
On Disconnection Value:	0 (0x0)
Password:	<Not Configured>
Prompt for Password:	Off

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

2. Enter or modify the following settings:

Tunnel - Accept Mode Page Settings	Description
<b>Mode</b>	<p>Select the method used to start a tunnel in Accept mode. Choices are:</p> <p><b>Disabled</b> = do not accept an incoming connection.</p> <p><b>Enabled</b> = accept an incoming connection. (<i>default</i>)</p> <p><b>Any Character</b> = start waiting for an incoming connection when any character is read on the serial line.</p> <p><b>Start Character</b> = start waiting for an incoming connection when the start character for the selected tunnel is read on the serial line.</p> <p><b>Modem Control Asserted</b> = start waiting for an incoming connection as long as the Modem Control pin (DSR) is asserted on the serial line until a connection is made.</p> <p><b>Modem Emulation</b> = start waiting for an incoming connection when triggered by modem emulation AT commands. Connect mode must also be set to <b>Modem Emulation</b>.</p>
<b>Local Port</b>	Enter the port number for use as the local port. The defaults are port <b>10001</b> for Tunnel 1 and port <b>10002</b> for Tunnel 2.
<b>Protocol</b>	Select the protocol type for use with Accept Mode. The default protocol is <b>TCP</b> .
<b>Flush Serial Data</b>	Select <b>Enabled</b> to flush the serial data buffer on a new connection.
<b>Block Serial Data</b>	Select <b>On</b> to block, or not tunnel, serial data transmitted to the MatchPort b/g Pro.
<b>Block Network Data</b>	Select <b>On</b> to block, or not tunnel, network data transmitted to the MatchPort b/g Pro.
<b>TCP Keep Alive</b>	Enter the time, in milliseconds, the MatchPort b/g Pro 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.
<b>Email on Connect</b>	Select whether the MatchPort b/g Pro sends an email when a connection is made. Select <b>None</b> if you do not want to send an email. Select <b>Email #</b> to send an email corresponding to the tunnel number.
<b>Email on Disconnect</b>	Select MatchPort b/g Pro sends an email corresponding to the tunnel number when a connection is closed. Select <b>None</b> if you do not want to send an email. Select <b>Email #</b> to send an email corresponding to the tunnel number.
<b>CP Set Group</b>	Identifies a CP or CP Group whose value should change when a connection is established and dropped.
<b>On Connection</b>	Specifies the value to set the CP or CP Group when a connection is established.
<b>On Disconnection</b>	Specifies the value used when the connection is closed.

Tunnel - Accept Mode Page Settings	Description
<b>Password</b>	<p>Enter a password that clients must send to the MatchPort b/g Pro within 30 seconds from opening a network connection to enable data transmission.</p> <p>The password can have up to 31 characters and must contain only alphanumeric characters and punctuation. When set, the password sent to the MatchPort b/g Pro must be terminated with one of the following: (a) <b>0x10 (LF)</b>, (b) <b>0x00</b>, (c) <b>0x13 0x10 (CR LF)</b>, or (d) <b>0x13 0x00</b>.</p>
<b>Prompt for Password</b>	<p>Indicate whether to prompt the user for the password upon connection.</p> <p><b>On</b> = prompt for a password upon connection.</p> <p><b>Off</b> = do not prompt for a password upon connection.</p>

- Click **Submit**. Changes are applied immediately to the MatchPort b/g Pro.

## Packing Mode

When in Packing Mode, data is not transferred one byte at a time. Instead, data is queued and sent in segments.

### To configure the tunnel's Packing Mode:

- Select **Tunnel 1** and **Packing Mode** at the top of the page. The Tunnel 1 Packing Mode page displays.

Figure 6-6. Tunnel 1 Packing Mode

Tunnel 1

Tunnel 2

Statistics

Serial Settings

Start/Stop Chars

Accept Mode

Connect Mode

Disconnect Mode

Packing Mode

Modem Emulation

AES Keys

### Tunnel 1- Packing Mode

**Mode:**
☐ Disabled
 ☐ Timeout
   
☐ Send Character

**Timeout:**  milliseconds

**Threshold:**

**Send Character:**

**Trailing Character:**

---

**Current Configuration**

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

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

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

**Disabled:** data never packed

**Timeout:** data sent after timeout occurs

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

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

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

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

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

- Enter or modify the following settings:

Tunnel - Packing Mode Page Settings	Description
<b>Mode</b>	Select <b>Disabled</b> to disable Packing Mode completely. Select <b>Send Character</b> to send the queued data when the send character is received. Select <b>Timeout</b> to send data after the specified time has elapsed.
<b>Timeout</b>	Enter a time, in milliseconds, for the MatchPort b/g Pro to send the queued data.
<b>Threshold</b>	Send the queued data when the number of queued bytes reaches the threshold.
<b>Send Character</b>	Enter the send character. Upon receiving this character, the MatchPort b/g Pro sends out the queued data.
<b>Trailing Character</b>	Enter the trailing character. This character is sent immediately following the send character.

- Click **Submit**. Changes are applied immediately to the MatchPort b/g Pro.

## Serial Settings

This page shows the settings for the tunnel selected at the top of the page and lets you change the settings.

**To configure serial settings:**

- Click **Tunnel 1** and **Serial Settings** at the top of the page. The Tunnel 1 Serial Settings page displays.

**Figure 6-7. Tunnel 1 Serial Settings**

Tunnel 1

Tunnel 2

Statistics

Serial Settings

Start/Stop Chars

Accept Mode

Connect Mode

Disconnect Mode

Packing Mode

Modem Emulation

AES Keys

### Tunnel 1- Serial Settings

<b>Line Settings:</b>	RS232, 9600, N, 8, 1, None
<b>Protocol:</b>	Tunnel
<b>Buffer Size:</b>	<input type="text" value="2048"/> bytes
<b>Wait Read Timeout:</b>	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
<b>Read Timeout:</b>	<input type="text" value="200"/> milliseconds
<b>DTR:</b>	<input checked="" type="radio"/> Asserted while connected <input type="radio"/> Continuously asserted

For Tunneling, the **Buffer Size** of the buffer used for reading data on the Serial Line can be modified. The valid size range is from 1 to 4096 bytes. Changing this value requires a reboot.

Enabling **Wait Read Timeout** specifies to wait the entire **Read Timeout** milliseconds from receipt of the first buffered character from the Serial Line before forwarding buffered data to the network. If the buffer fills before the **Read Timeout** elapses, the buffer is forwarded immediately.

The **DTR** option **Asserted while connected** causes DTR to be asserted whenever either a connect or an accept mode tunnel connection is active.

- View or modify the following settings:

Tunnel - Serial Settings Page Settings	Description
<b>Line Settings</b> (display only)	Current serial settings for the line.

Tunnel - Serial Settings Page Settings	Description
<b>Protocol</b> (display only)	The protocol being used on the line, in this case, <b>Tunnel</b> .
<b>Buffer Size</b>	Enter the buffer size used for the tunneling of data received. Requires reboot to take effect.
<b>Read Timeout</b>	Enter the maximum number of milliseconds that the MatchPort waits for incoming data on the serial line. Default is 200 milliseconds.
<b>Wait for Read Timeout</b>	<p>Select whether the MatchPort waits the entire <b>Read Timeout</b> value for incoming data on the serial line. Waiting occurs even if there is data in the read buffer ready to be processed. The Read Timeout is ignored only when the read buffer completely fills with data. Choices are:</p> <p><b>Enabled</b> = waits the entire <b>Read Timeout</b> value for incoming data on the serial line.</p> <p><b>Disabled</b> = does not wait the entire <b>Read Timeout</b> value for incoming data (<i>default</i>).</p>
<b>DTR</b>	<p>Select when to assert DTR.</p> <p><b>Asserted while connected</b> = asserted whenever either a connect or an accept mode tunnel connection is active.</p> <p><b>Continuously asserted</b> = asserted regardless of the status of a tunnel connection.</p>

3. In the **Current Configuration** table, reset currently stored settings as necessary.
4. Click **Submit**. Changes are applied immediately to the MatchPort b/g Pro.

## Connect Mode

Connect mode defines how the unit makes an outgoing connection.

### To configure Tunnel 1's Connect Mode:

1. Select **Tunnel 1** and **Connect Mode** at the top of the page. The Tunnel 1 Connect Mode page displays.

Figure 6-8. Tunnel 1 Connect Mode

Tunnel 1
Tunnel 2

Statistics  
 Accept Mode  
 Packing Mode

Serial Settings  
Connect Mode  
 Modem Emulation

Start/Stop Chars  
 Disconnect Mode  
 AES Keys

### Tunnel 1- Connect Mode

Mode: ☐ Disabled ☐ Enabled

☐ Any Character
☐ Modem Control Asserted
☐ Start Character
☐ Modem Emulation

Remote Address:

Remote Port:

Local Port:

Protocol: ☐ TCP ☐ UDP ☐ SSH  
☐ TCP/AES ☐ UDP/AES

Reconnect Timer:  milliseconds

Flush Serial Data: ☐ Enabled ☐ Disabled

SSH Username:

Block Serial Data: ☐ On ☐ Off

Block Network Data: ☐ On ☐ Off

TCP Keep Alive:  seconds

Email on Connect: None ▼

Email on Disconnect: None ▼

CP Set Group:

On Connection:

On Disconnection:

Submit

#### Current Configuration

Mode:	Disabled
Remote Address:	<None>
Remote Port:	<None>
Local Port:	Random
Protocol:	Tcp
Reconnect Timer:	15000milliseconds
Flush Serial Data:	Disabled
SSH Username:	<None>
Block Serial Data:	Off
Block Network Data:	Off
TCP Keep Alives:	Default 45 seconds
Email on Connect:	<None>
Email on Disconnect:	<None>
CP Set Group:	<None>
On Connection Value:	0 (0x0)
On Disconnection Value:	0 (0x0)

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

**Disabled:** never started

**Enabled:** always started

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

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

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

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

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

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

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

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

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

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

The **CP Set Group** identifies a CP or CP Group whose value should change when a connection is established and dropped. **On Connection** specifies the value to set the CP or CP Group to when a connection is established and **On Disconnection** specifies the value that should be used when the connection is closed.



2. Enter or modify the following settings:

Tunnel – Connect Mode Page Settings	Description
<b>Mode</b>	<p>Select the method to be used to attempt a connection to a remote host or device. Choices are:</p> <p><b>Disabled</b> = an outgoing connection is never attempted. (default)</p> <p><b>Enabled</b> = a connection is attempted until one is made. If the connection gets disconnected, the MatchPort b/g Pro retries until a connection it makes a connection.</p> <p><b>Any Character</b> = a connection is attempted when any character is read on the serial line.</p> <p><b>Modem Control Asserted</b> = a connection is attempted as long as the Modem Control pin (DSR) is asserted until a connection is made.</p> <p><b>Start Character</b> = a connection is attempted when the start character for the selected tunnel is read on the serial line.</p> <p><b>Modem Emulation</b> = a connection is attempted when triggered by modem emulation AT commands.</p>
<b>Remote Address</b>	Enter the remote address to which the MatchPort b/g Pro will connect. Enter an IP address or DNS name.
<b>Remote Port</b>	Enter the remote port number.
<b>Local Port</b>	Enter the port for use as the local port. A random port is selected by default. Once you have configured a number, click the <b>Random</b> link in the Current Configuration to switch back to random.
<b>Protocol</b>	<p>Select the protocol type for use in Command Mode. TCP is the default protocol.</p> <p>The protocol used on the connection can be one of TCP, UDP, SSH, SSL, Telnet, TCP w/AES, or UDP w/AES.</p> <p>If security is a concern, we recommend using SSH. The <b>SSH Username</b> specifies the SSH Client User to use for an outgoing SSH connection. To set up an SSH Client User, go to the, go to <a href="#">SSH Settings</a> on page 94.</p>
<b>Reconnect Timer</b>	Enter the reconnect time in milliseconds. The MatchPort b/g Pro attempts to reconnect after this amount of time after failing a connection or exiting an existing connection.
<b>Flush Serial Data</b>	<p>Select whether to flush the serial line when a connection is made. Choices are:</p> <p><b>Enabled</b> = flush the serial line when a connection is made.</p> <p><b>Disabled</b> = do not flush the serial line. (default)</p>
<b>SSH Username</b>	Enter the SSH username. The tunnel uses the SSH keys for the client username.
<b>Block Serial Data</b>	Select <b>On</b> to block (not tunnel) serial data transmitted to the MatchPort b/g Pro.
<b>Block Network Data</b>	Select <b>On</b> to block (not tunnel) network data transmitted to the MatchPort b/g Pro.

Tunnel – Connect Mode Page Settings	Description
<b>TCP Keep Alive</b>	Enter the time, in milliseconds, the unit waits during a silent connection before checking whether the currently connected network device is still on the network. If the unit then gets no response after 8 attempts, it drops that connection.
<b>Email on Connect</b>	Select whether the MatchPort b/g Pro sends an email when a connection is made. Select <b>None</b> if you do not want to send an email. Select <b>Email #</b> to send an email corresponding to the tunnel number.
<b>Email on Disconnect</b>	Select whether the MatchPort b/g Pro sends an email corresponding to the tunnel number when a connection is closed. Select <b>None</b> if you do not want to send an email. Select <b>Email #</b> to send an email corresponding to the tunnel number.
<b>CP Set Group</b>	Identifies a CP or CP Group whose value should change when a connection is established and when it is dropped.
<b>On Connection</b>	Specifies the value to set the CP or CP Group when a connection is established.
<b>On Disconnection</b>	Specifies the value used when the connection is closed.

- Click **Submit**. Changes are applied immediately to the MatchPort b/g Pro.

## 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 1 or Tunnel 2 Connect Mode type.

### To configure modem emulation:

- Select **Tunnel 1** and then **Modem Emulation** at the top of the page. The Tunnel 1 Modem Emulation page displays.

Figure 6-9. Tunnel 1 Modem Emulation

Tunnel 1
Tunnel 2

**Statistics**  
Accept Mode  
Packing Mode

**Serial Settings**  
Connect Mode  
**Modem Emulation**

**Start/Stop Chars**  
Disconnect Mode  
AES Keys

### Tunnel 1- Modem Emulation

Echo Pluses: ☒ On ☐ Off  
Echo Commands: ☒ On ☐ Off  
Verbose Response Codes: ☒ On ☐ Off  
Response Codes: ☒ Text ☐ Numeric  
Error Unknown Commands: ☒ On ☐ Off  
Connect String:

#### Current Configuration

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

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

The **Echo Pluses** specifies that pluses will be sent into the network (rather than suppressed) after a "pause +++ pause" escape sequence is seen on the Serial Line.

The **Echo Commands** specifies that characters read on the Serial Line will be echoed while the Line is in Modem Command Mode.

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

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

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

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

2. Enter or modify the following settings:

Tunnel- Modem Emulation Page Settings	Description
<b>Echo Pluses</b>	Select <b>On</b> to echo +++ when entering modem Command Mode.
<b>Echo Commands</b>	Select <b>On</b> to echo the modem commands to the console.
<b>Verbose Response Codes</b>	Select <b>On</b> to send modem response codes out on the serial line.
<b>Response Codes</b>	Select the type of response code from either <b>Text</b> or <b>Numeric</b> .
<b>Error Unknown Commands</b>	<p>Select whether an <b>ERROR</b> or <b>OK</b> response is sent in reply to unrecognized AT commands. Choices are:</p> <p><b>On</b> = <b>ERROR</b> is returned for unrecognized AT commands.</p> <p><b>Off</b> = <b>OK</b> is returned for unrecognized AT commands. (default)</p>
<b>Connect String</b>	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.

3. Click **Submit**. Changes are applied immediately to the MatchPort b/g Pro.

## Start and Stop Characters

The Start/Stop Chars page enables you to configure the MatchPort b/g Pro to start a tunnel when it receives a specific start character from the serial port and to disconnect upon receiving the stop character.

To configure the start and stop characters mode:

1. Select **Tunnel 1** and **Start/StopChars** at the top of the page. The Tunnel 1 Start/Stop Chars page displays.

Figure 6-10. Tunnel 1 Start/Stop Chars

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

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

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

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

2. Enter or modify the following settings:

Tunnel – Start/Stop Chars Page Settings	Description
<b>Start Character</b>	Enter the start character in either ASCII or hexadecimal notation.
<b>Stop Character</b>	Enter the stop character in either ASCII or hexadecimal notation.
<b>Echo Start Character</b>	Select <b>On</b> to forward (tunnel) the start character.
<b>Echo Stop Character</b>	Select <b>On</b> to forward (tunnel) the stop character.

3. Click **Submit**. Changes are applied immediately to the MatchPort b/g Pro.

## Disconnect Mode

Disconnect Mode is disabled by default. When enabled, Disconnect Mode runs in the background of an active connection to determine when a disconnection is required.

**To configure the tunnel's Disconnect Mode:**

1. Click **Tunnel 1** and **Disconnect Mode** at the top of the page. The Tunnel 1 Disconnect Mode page displays.

**Figure 6-11. Tunnel 1 Disconnect Mode**

These settings relate to Disconnecting a Tunnel.

**Character Stop** enables disconnect when the "Stop Character" (configured on the "Start/Stop Chars" page) is read on the Serial Line.

**Modem Control** enables disconnect when the Modem Control pin is not asserted on the Serial Line.

**Timeout** enables disconnect after the tunnel is idle for a specified number of milliseconds. The value of zero disables the idle timeout.

**Flush Serial Data** enabled will flush the Serial Line when the Tunnel is disconnected.

Tunnel 1		Tunnel 2
Statistics	Serial Settings	Start/Stop Chars
Accept Mode	Connect Mode	<b>Disconnect Mode</b>
Packing Mode	Modem Emulation	AES Keys

### Tunnel 1- Disconnect Mode

Character Stop:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Modem Control:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Timeout:	<input type="text" value="0"/> milliseconds
Flush Serial Data:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled

2. Enter or modify the following settings:

Tunnel – Disconnect Mode Page Settings	Description
<b>Character Stop</b>	Select <b>Enabled</b> to disconnect upon receiving the stop character. (See <a href="#">Start and Stop Characters</a> on page 68 for instructions on configuring the stop character.)
<b>Modem Control</b>	Select <b>Enabled</b> to disconnect when the modem control pin is not asserted on the serial line.
<b>Timeout</b>	Enter a time, in milliseconds, for the MatchPort b/g Pro to disconnect on a timeout. The value 0 (zero) disables the idle timeout.
<b>Flush Serial Data</b>	Select <b>Enabled</b> to flush the serial data buffer on a disconnection.

3. Click **Submit**. Changes are applied immediately to the MatchPort b/g Pro.

**AES Keys**

Advanced Encryption Standard (AES) is an encryption algorithm for securing sensitive information by government agencies.

**To configure the AES keys for connect or Accept Mode:**

1. Click **Tunnel 1** and **AES Keys** at the top of the page. The Tunnel 1 AES Keys page displays.

Figure 6-12. AES Keys

**Tunnel 1** Tunnel 2

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

### Tunnel 1- AES Keys

**Accept Mode AES Keys**

Encrypt Key:  ☒ Text ☐ Binary

Decrypt Key:  ☒ Text ☐ Binary

**Connect Mode AES Keys**

Encrypt Key:  ☒ Text ☐ Binary

Decrypt Key:  ☒ Text ☐ Binary

**Current Configuration**

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

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

There are four separate Advanced Encryption Standard (AES) Encryption Keys used for Tunneling. Connect Mode and Accept Mode contain their own sets of keys. One Key is used for encrypting outgoing data and the other Key is used for decrypting incoming data.

These AES Keys are a fixed 16 bytes in length. Any Keys entered that are less than 16 bytes long are padded with zeroes. Key data can be entered in as **Text** or **Binary** form. The **Text** form is a simple string of ASCII characters. **Binary** form is a string of characters representing byte values where each Hexadecimal byte value starts with 0x and each Decimal byte value starts with \.

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

Note that this device also supports SSH using AES Encryption as an alternative to secure tunneling. It is recommended that SSH be used because it does not require configuring shared secret keys and is a more secure standards based protocol. [SSH](#).

- Enter or modify the following settings:

#### Tunnel – AES Keys Page Description Settings

##### Accept Mode AES Keys

**Encrypt Key** Enter the value for each byte of the encryption key. Select the format for the byte as either **Text** or **Binary**. Binary form is a string of characters representing byte values where each hexadecimal byte value starts with **0x** and each decimal byte value starts with **\**.  
*Note: Empty trailing bytes that are not specified are set to 0.*

**Decrypt Key** Enter the value for each byte of the decrypt key. Select the format for the bytes as either **Text** or **Binary**.  
*Note: Empty trailing bytes that are not specified are set to 0.*

##### Connect Mode AES Keys

**Encrypt Key** Enter the value for each byte. Select the format for the byte as either **Text** or **Binary**. Trailing bytes not specified are set to 0.

**Decrypt Key** Enter the value for each byte of the decrypt key. Select the format for the byte as either **Text** or **Binary**.  
*Note: Empty trailing bytes that are not specified are set to 0.*

- Click **Submit**. Changes are applied immediately to the MatchPort b/g Pro.

## Terminal Settings

This page displays configuration settings for attaching a terminal on a serial line or the network and lets you change them as necessary.

### Line Terminal Configuration

To configure a line to support an attached terminal:

1. Click **Terminal** on the menu and then select the line that is connected to the terminal you want to configure. The default is **Line 1**. Configuration is automatically selected. The Terminal on Line 1 Configuration page displays.

Figure 6-13. Terminal on Line 1 Configuration

Terminal on Line 1- 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
Send Break:	<input type="text"/>
Break Duration:	500 milliseconds
Echo:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled

The text in **Terminal Type** will be sent to a host via IAC.

Selecting **Login Connect Menu** will bring the user to a menu rather than to the command line interface (CLI) upon logging in.

Selecting **Exit Connect Menu** allows a user to reach the command line interface (CLI) from the Connect Menu.

When the **Send Break** control character is received from the network on its way to a Serial Line, it will not be sent to the Line; instead, the line output will be forced inactive. Example setting: <control>Y

The **Break Duration** specifies how long the "spacing" condition will be placed on the line when a break is sent.

**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.

2. Enter or modify the following settings:

Terminal on Line Configuration Page Settings	Description
Terminal Type	Enter text to describe the type of terminal. The text will be sent to a host via IAC. <b>Note:</b> 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:  <b>Enabled</b> = displays the Login Connect Menu. <b>Disabled</b> = displays the CLI

Terminal on Line Configuration Page Settings	Description
<b>Exit Connect Menu</b>	Select whether to display a choice for the user to exit the Login Connect Menu and reach the CLI. Choices are:  <b>Enabled</b> = a choice allows the user to exit to the CLI.  <b>Disabled</b> = there is no exit to the CLI.
<b>Send Break</b>	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).
<b>Break Duration</b>	Enter how long the break should last in milliseconds.
<b>Echo</b>	Applies only to Connect Mode Telnet connections, not to Accept Mode. Only disable <b>Echo</b> if your terminal echoes, in which case you will see double of each character typed.

- To save changes, click **Submit**. Changes are applied immediately to the MatchPort b/g Pro.

## Network Terminal Configuration

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

- Click **Terminal** on the menu and then click **Network** at the top of the page. Configuration is automatically selected. The Terminal on Network Configuration page displays.

Figure 6-14. Terminal on Network Configuration

The text in **Terminal Type** will be sent to a host via IAC.

Selecting **Login Connect Menu** will bring the user to a menu rather than to the command line interface (CLI) upon logging in.

Selecting **Exit Connect Menu** allows a user to reach the command line interface (CLI) from the Connect Menu.

When the **Send Break** control character is received from the network on its way to a Serial Line, it will not be sent to the Line; instead, the line output will be forced inactive. Example setting: <control>Y

The **Break Duration** specifies how long the "spacing" condition will be placed on the line when a break is sent.

**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.

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

- Enter or modify the following settings:



Terminal on Line Configuration Page Settings	Description
<b>Terminal Type</b>	Enter text to describe the type of terminal. The text will be sent to a host via IAC. <b>Note:</b> IAC means, "interpret as command." It is a way to send commands over the network such as <code>send break</code> or <code>start echoing</code> .
<b>Login Connect Menu</b>	Select the interface to display when the user logs in. Choices are:  <b>Enabled</b> = displays the Login Connect Menu. <b>Disabled</b> = displays the CLI
<b>Exit Connect Menu</b>	Select whether to display a choice for the user to exit the Login Connect Menu and reach the CLI. Choices are:  <b>Enabled</b> = a choice allows the user to exit to the CLI. <b>Disabled</b> = there is no exit to the CLI.
<b>Echo</b>	Applies only to Connect Mode Telnet connections, not to Accept Mode. Only disable <b>Echo</b> if your terminal echoes, in which case you will see double of each character typed.

- To save changes, click **Submit**. Changes are applied immediately to the MatchPort b/g Pro.

## Host Configuration

This page displays current settings for a remote host and lets you change these settings.

- Click **Host** on the menu and then click the desired host at the top of the page. Configuration is automatically selected. (Host 1 is the default.) Host Configuration page displays.

Figure 6-15. Host Configuration

The screenshot shows the 'Host Configuration' page. At the top, there are tabs for 'Host 1' and 'Host 2', with 'Host 1' selected. Below the tabs is a 'Configuration' button. The main section is titled 'Host 1- Configuration'. It contains a form with the following fields:

- Name:** A text input field.
- Protocol:** Radio buttons for 'Telnet' (selected) and 'SSH'.
- Remote Address:** A text input field.
- Remote Port:** A text input field with the value '0'.

On the right side of the form, there is a text box with the following instructions:

The text in **Name** will appear in the connect menu. Set it blank to leave it out of the menu.

If **Protocol** is SSH, either supply a value in **SSH Username** to select a pre-configured Username / Password / Key (in SSH Client: Users) or leave it blank to be prompted for Username and Password at connect time.

The **Remote Address** and **Remote Port** specify the remote host to connect to.

- Enter or modify the following settings:

## Host Page

Host Page Settings	Description
Name	Enter a name for the host. This name displays on the Login Connect Menu. To leave a host out of the menu, leave this field blank.
Protocol	<p>Select the protocol to use to connect to the host. Choices are:</p> <p><b>Telnet</b></p> <p><b>SSH</b></p> <p><i><b>Note:</b> SSH keys must be loaded or created on the SSH page for the SSH protocol to work.</i></p>
SSH Username	Displays if you selected <b>SSH</b> 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.
Remote Port	Enter the port on the host to which the MatchPort will connect.

- To save changes, click **Submit**. Changes are applied immediately to the MatchPort b/g Pro.

## 7: Configuration Pin Manager

The Configurable Pin Manager is responsible for assignment and control of the configurable pins (CPs) available on the MatchPort b/g Pro. There are seven configurable pins on the MatchPort b/g Pro.

You can configure the CPs individually or cluster them together and configure them as a single group (CP group). This increases flexibility when incorporating the MatchPort b/g Pro into another system.

### Configurable Pin Manager

The MatchPort b/g Pro has seven configurable pins (CPs). CPs can be grouped together using the Configurable Pin Manager (CPM).

#### CPM: Configurable Pins

Each CP is associated with an external hardware pin. CPs can trigger an outside event, such as sending an email message or starting Command Mode.

#### To configure the MatchPort b/g Pro's CPs:

1. Click **CPM** on the menu bar and then **CPs** at the top of the page. The CPM: CPs page displays.

### Figure 7-1. CPM: CPs

CPs

Groups

## CPM: CPs

### Current Configuration

CP	Pin #	Configured As	State	Groups	Active In Group
<u>CP1</u>	CP1	Input	0	0	<available>
<u>CP2</u>	CP2	Input	0	0	<available>
<u>CP3</u>	CP3	Input	0	0	<available>
<u>CP4</u>	CP4	Input	0	0	<available>
<u>CP5</u>	CP5	Input	0	0	<available>
<u>CP6</u>	CP6	Input	0	0	<available>
<u>CP7</u>	CP7	Input	0	0	<available>

### CP Status: CP1

Name	CP01																																						
State	Enabled																																						
Type	Input																																						
Value	0 (0x0)																																						
Bit	3	3	2	2	2	2	2	2	2	2	2	2	2	2	1	1	1	1	1	1	1	1	1	1	1	1	1	9	8	7	6	5	4	3	2	1	0		
Level	1	0	9	8	7	6	5	4	3	2	1	0	9	8	7	6	5	4	3	2	1	0	9	8	7	6	5	4	3	2	1	0							
I/O																																							
Logic																																							
Binary	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	0	
CP#																																						1	
Groups																																							

Set

CP1

to value

Submit

Set

CP1

as

Input

☐ Assert Low

Submit

This page allows you to manage the **Configurable Pins (CP)** on the device. CPs can be grouped together and based on their state, can trigger an outside event like sending an Email message or starting the CLI on a Serial Line.

Each CP is associated with an external hardware pin and can be configured in either **input** or **output** mode. When a CP is configured as **output**, it can be toggled by setting the value. Whatever value is given, the first bit is used as the setting. 1 means asserted and 0 means de-asserted. Additionally, the CP logic can be **inverted** so that assertion is low.

A CP can be a member of multiple groups but can only be a member of one enabled group. Note that a CP can only be modified if all the groups it is a member of are disabled.

The Pin Status chart shows the current status for an individual CP. A CP contains one bit of information and the **Value** shows the current value. The **Level** row shows the voltage as 'H' for high and 'L' for low. The **I/O** row shows input 'I', output 'O', or not available 'X'. An 'I' in the **Logic** row means the CP is inverted. Lastly, a listing is shown of all groups the CP is a member of.

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

## Current Configuration

CPM – CPs Page Current Configuration	Description
CP	Indicates the configurable pin number.
Pin #	Indicates the hardware pin number associated with the CP.
Configured As	Displays the CP's configuration. A CP configured as <b>Input</b> is set to read input. A CP configured as <b>Output</b> drives data out of the MatchPort b/g Pro.
State	Indicates the current status of the CP:  1 = asserted.  0 = de-asserted.  I = the CP is inverted.
Groups	Indicates the number of groups in which the CP is a member.
Active In Group	A CP can be a member of several groups. However, it may only be active in one group. This field displays the group in which the CP is active.

2. To display the CP status of a specific pin, click the CP number in the Current Configuration table. The CP Status table displays detailed information about the CP.

CPM – CPs Page CP Status	Description
<b>Name</b>	Displays the CP number.
<b>State</b>	Displays the current enable state of the CP.
<b>Type</b>	Indicates whether the CP is set for input or output.
<b>Value</b>	Displays the last bit in the CP's current value.
<b>Bit</b>	Visual display of the 32 bit placeholders for a CP.
<b>Level</b>	A "+" symbol indicates the CP is asserted (the voltage is high). A "-" indicates the CP voltage is low.
<b>I/O</b>	Indicates the current status of the pin:  I = input  O = output  X = unassigned
<b>Logic</b>	An "I" indicates the CP is inverted.
<b>Binary</b>	Displays the assertion value of the corresponding bit.
<b>CP#</b>	Displays the CP number.
<b>Groups</b>	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.

3. To change a CP's value:
  - a) Select the CP from the drop-down list.
  - b) Enter the CP's value.
  - c) Click **Submit**. Changes are applied immediately to the MatchPort b/g Pro.
4. To change a CP's configuration:
  - a) Select the CP from the drop-down list.
  - b) Select the CP's configuration from the drop-down list.
  - c) (If necessary) Select the **Assert Low** checkbox.
  - d) Click **Submit**. Changes are applied immediately to the MatchPort b/g Pro.

## CPM: Groups

The CP Groups page allows for the management 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.

### To configure the MatchPort b/g Pro's CP groups:

1. Click **CPM** on the menu bar and then **Groups** at the top of the page. The CPM: Groups page displays.

### Figure 7-2. CPM: Groups

CPs

Groups

## CPM: Groups

### Current Configuration

Group Name	State	CP Info
<a href="#">Line2_Modem_Ctl_O</a>	Disabled	0 CPs Assigned
<a href="#">Line1_RS485_HDpx</a>	Disabled	0 CPs Assigned
<a href="#">Line2_Modem_Ctl_In</a>	Disabled	0 CPs Assigned
<a href="#">Line1_Modem_Ctl_O</a>	Disabled	0 CPs Assigned
<a href="#">Line1_RS485_Select</a>	Disabled	0 CPs Assigned
<a href="#">Line1_Modem_Ctl_In</a>	Disabled	0 CPs Assigned

### Group Status: Line2\_Modem\_Ctl\_O

Name	Line2_Modem_Ctl_O																																			
State	Disabled AND Locked, user may Enable/Disable or Add/Remove CP																																			
Value	Disabled																																			
Bit	3	3	2	2	2	2	2	2	2	2	2	2	2	1	1	1	1	1	1	1	1	1	1	1	1	1	9	8	7	6	5	4	3	2	1	0
Level	1	0	9	8	7	6	5	4	3	2	1	0	9	8	7	6	5	4	3	2	1	0	9	8	7	6	5	4	3	2	1	0				
I/O																																				
Logic																																				
Binary	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	
CP#																																				

Create Group:

Submit

Delete Group:

Line2\_Modem\_Ctl\_O

Submit

Set

Line2\_Modem\_Ctl\_O

state to

Enabled

Submit

Set

Line2\_Modem\_Ctl\_O

to value

Submit

Add

CP1

to

Line2\_Modem\_Ctl\_O

bit

Next

Submit

Remove

CP1

from

Line2\_Modem\_Ctl\_O

Submit

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

### Current Configuration

CPM – Groups Page Current Configuration	Description
<b>Group Name</b>	Displays the CP group's name.
<b>State</b>	Indicates whether the group is enabled or disabled.
<b>CP Info</b>	Provides CP group information.

- To display the status of a specific group, click the CP group name in the Current Configuration table. The Group Status table displays, providing detailed information about the CP group.

### Group Status

CPM – Groups Page Group Status	Description
<b>Name</b>	Displays the CP Group name.
<b>State</b>	Current enable state of the CP group.
<b>Value</b>	Displays the CP group's current value.
<b>Bit</b>	Visual display of the 32 bit placeholders for a CP.
<b>Level</b>	A "+" symbol indicates the CP's bit position is asserted (the voltage is high). A "-" indicates the CP voltage is low.
<b>I/O</b>	Indicates the current status of the pin:  I = input  O = output  X = unassigned
<b>Logic</b>	An "I" indicates the CP is inverted.
<b>Binary</b>	Displays the assertion value of the corresponding bit.
<b>CP#</b>	Displays the configurable pin number and its bit position in the CP group.

#### To create a CP group:

- Enter a group name in the **Create Group** field.
- Click **Submit**. Changes are applied immediately to the MatchPort b/g Pro.

#### To delete a CP group:

- Select the CP group from the **Delete Group** drop-down list.
- Click **Submit**. Changes are applied immediately to the MatchPort b/g Pro.

#### To enable or disable a CP group:

- Select the CP group from the **Set** drop-down list.
- Select the state (**Enabled** or **Disabled**) from the drop-down list.
- Click **Submit**. Changes are applied immediately to the MatchPort b/g Pro.

**To set a CP group's value:**

1. Select the CP group from the **Set** drop-down list.
2. Enter the CP group's value in the **value** field.
3. Click **Submit**. Changes are applied immediately to the MatchPort b/g Pro.

**To add a CP to a CP group:**

1. Select the CP from the **Add** drop-down list.
2. Select the CP group from the drop-down list.
3. Select the CP's bit location from the **bit** drop-down list.
4. Click **Submit**. Changes are applied immediately to the MatchPort b/g Pro.

**To delete a CP from a CP group:**

1. Select the CP from the **Remove** drop-down list.
2. Select the CP group from the drop-down list.
3. Click **Submit**. Changes are applied immediately to the MatchPort b/g Pro.



## 8: Services Settings

### DNS Configuration

This page displays configuration settings for the domain name system (DNS). The primary and secondary 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 page also shows any contents in the DNS cache. When a DNS name is resolved using a forward lookup, the results are stored in the DNS cache temporarily. The MatchPort b/g Pro consults this cache when performing forward lookups. Each item in the cache eventually times out and is removed automatically after a certain period, or you can delete it manually.

**To configure the MatchPort b/g Pro's DNS configuration:**

1. Click **DNS** on the menu bar. The DNS page displays.

**Figure 8-1. DNS Settings**

DNS	
<b>Current Status</b>	
Primary DNS:	<None>
Secondary DNS:	<None>
<b>DNS Cache</b>	
There are no entries in the cache.	

This page displays the current status of the DNS subsystem. The primary and secondary DNS addresses come from the active interface. The static addresses from the Network Interface Configuration page may be overridden by DHCP or BOOTP.  
When a DNS name is resolved using a forward lookup, the results are temporarily stored in the DNS cache. This cache is consulted first when performing forward lookups. Each item in the cache will eventually timeout and be removed after a certain period of time or can be deleted manually.

### PPP Configuration

Point-to-Point Protocol (PPP) establishes a direct connection between two nodes. It defines a method for data link connectivity between devices using physical layers (such as serial lines). For more information about PPP, see [12: Point-to-Point Protocol \(PPP\)](#).

The MatchPort b/g Pro supports two types of PPP authorization: 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 supports no authentication scheme when no authentication is required during link negotiation.

**Note:** The following section describes the steps to configure PPP 1 (PPP on serial line 1); these steps also apply to PPP 2. You must use static routes to configure PPP.

**To configure the MatchPort b/g Pro's PPP configuration:**

1. Click **PPP** on the menu bar and **Line1** at the top of the page. The PPP – Line 1 page displays.

**Figure 8-2. PPP Settings**

**PPP: Line 1**

Local IP Address:

Peer IP Address:

Network Mask:

Auth Mode: ☐ None ☐ PAP ☐ CHAP

Auth Username:

Auth Password:

**Current Configuration**

Mode:	Disabled
Local IP Address:	<None>
Peer IP Address:	<None>
Network Mask:	<None>
Auth Mode:	None
Auth Username:	<None>
Auth Password:	<None>

This page is used to configure a network link using PPP over a serial line. In order to enable PPP, no other features can be enabled on the serial line. Tunneling (Connect and Accept modes) and Command Mode must both be turned off before proceeding.

It's important to note that this device acts as the server side of the PPP link. This device can force authentication and is able to assign an IP Address to the peer. Once the PPP interface is up, IP packets are routed appropriately to and from the Ethernet and PPP interfaces.

The **Local IP Address** is the IP Address that will be assigned to the PPP interface on the device. The **Peer IP Address** is the IP Address that will be assigned to the peer if asked during negotiation.

There are three different authentication schemes supported by this device. **None** which means no authentication is necessary during link negotiation, the **Password Authentication Protocol (PAP)** and **Challenge-Handshake Authentication Protocol (CHAP)**. **PAP** and **CHAP** require that a username and password be configured for the PPP interface.

The **Auth Username** and **Auth Password** are the credentials used by the **PAP** and **CHAP** authentication protocols during link negotiation. If authentication is to be used on the PPP interface, the peer must be configured to use this username and password.

2. Enter or modify the following settings:

PPP Page Settings	Description
<b>Local IP Address</b>	Enter the IP address assigned to the MatchPort b/g Pro's PPP interface.
<b>Peer IP Address</b>	Enter the IP address assigned to the peer (when requested during negotiation).
<b>Network Mask</b>	Enter the network mask.
<b>Auth. Mode</b>	Choose the authentication mode:  <b>None</b> = no authentication is required.  <b>PAP</b> = Password Authentication Protocol.  <b>CHAP</b> = Challenge Handshake Authentication Protocol.
<b>Auth. Username</b>	Enter the username if authentication is used on the PPP interface.
<b>Auth. Password</b>	Enter the password if authentication is used on the PPP interface.

3. Click **Submit**. Changes are applied immediately to the MatchPort b/g Pro

## SNMP Configuration

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

### To configure SNMP:

1. Click **SNMP** on the menu bar. The SNMP page opens and displays the current SNMP configuration.

Figure 8-3. SNMP Configuration

**SNMP**

This page displays the current configuration of the SNMP Agent.

SNMP Agent: ☒ On ☐ Off

Read Community:

Write Community:

System Contact:

System Name:

System Description:

System Location:

Enable Traps: ☒ On ☐ Off

Primary TrapDest IP:

Secondary TrapDest IP:

---

**Current Configuration**

SNMP Agent Status:	Running (On)
Read Community:	<Configured>[Delete]
Write Community:	<Configured>[Delete]
System Contact:	<None>
System Name:	matchport[Delete]
System Description:	Lantronix MatchPort AR[Delete]
System Location:	<None>
Traps Enabled:	On
Primary TrapDest IP:	<None>
Secondary TrapDest IP:	<None>

2. Enter or modify the following settings:

SNMP Page Settings	Description
<b>SNMP Agent</b>	Select <b>On</b> to enable SNMP.
<b>Read Community</b>	Enter the SNMP read-only community string.
<b>Write Community</b>	Enter the SNMP read/write community string.
<b>System Contact</b>	Enter the name of the system contact.
<b>System Name</b>	Enter the system name.
<b>System Description</b>	Enter the system description.
<b>System Location</b>	Enter the system location.
<b>Enable Traps</b>	Select <b>On</b> to enable the transmission of the SNMP cold start

	trap messages. This trap is generated during system boot.
<b>Primary TrapDest IP</b>	Enter the primary SNMP trap host.
<b>Secondary TrapDest IP</b>	Enter the secondary SNMP trap host.

3. In the **Current Configuration** table, delete and clear currently stored settings as necessary.
4. Click **Submit**. Changes are applied immediately to the MatchPort b/g Pro.

## FTP Configuration

This page displays the current File Transfer Protocol (FTP) connection status and various statistics about the FTP server.

### To configure FTP:

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

Figure 8-4. FTP Configuration

**FTP**

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

FTP Server: ☒ On ☐ Off

Username:

Password:

---

**Current FTP Configuration and Statistics**

FTP Status:	On (running)
FTP Username:	admin
FTP Password:	<Configured> <a href="#">Reset</a>
Connections Rejected:	0
Connections Accepted:	0
Active Connections:	0
Last Client:	No device has connected

2. Enter or modify the following settings:

FTP Page Settings	Description
<b>FTP Server</b>	Select <b>On</b> to enable the FTP server.
<b>Username</b>	Enter the username to use when logging in via FTP.
<b>Password</b>	Enter the password to use when logging in via FTP.

3. In the **Current FTP Configuration and Statistics** tables, reset currently stored settings as necessary by clicking the **Reset** link.
4. Click **Submit**. Changes are applied immediately to the MatchPort b/g Pro.

## TFTP Configuration

This page displays the status and various statistics about the Trivial File Transfer Protocol (TFTP) server.

### To configure TFTP:

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

Figure 8-5. TFTP Configuration

**TFTP**

TFTP Server: ☒ On ☐ Off

Allow TFTP File Creation: ☐ On ☒ Off

---

**Current TFTP Configuration and Statistics**

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

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

The **Allow TFTP File Creation** boolean specifies whether or not the TFTP Server can create a file if it does not already exist. Be careful when turning this feature on as it opens the device up to possible Denial-of-Service (DoS) attacks against the filesystem.

2. Enter or modify the following settings:

TFTP Page Settings	Description
<b>TFTP Server</b>	Select <b>On</b> to enable the FTP server.
<b>Allow TFTP File Creation</b>	Select whether to allow the creation of new files stored on the TFTP server.

3. In the **Current TFTP Configuration and Statistics** table, reset currently stored settings as necessary by clicking the **Reset** link.
4. Click **Submit**. Changes are applied immediately to the MatchPort b/g Pro.

## Syslog Configuration

The Syslog page shows the current configuration, status, and statistics of the syslog. Here you can configure the syslog destination and the severity of the events to log.

**Note:** The system log is always saved to local storage, but it is not retained through reboots. Saving the system log to a server that supports remote logging services (see RFC 3164) allows the administrator to save the complete system log history. The default is **514**.

1. Click **Syslog** on the menu bar. The Syslog page opens to display the current configuration.

Figure 8-6. Syslog

**Syslog**

Syslog: ☐ On ☐ Off

Host:

Local Port:

Remote Port:

Severity To Log: None

**Current Syslog Configuration and Statistics**

Syslog Status:	Off (not running)
Host:	<None>
Local Port:	514
Remote Port:	514
Severity Level:	<None>
Messages Sent:	0
Messages Failed:	0

This page displays the current configuration, status and various statistics for Syslog.

The **Severity To Log** field is used to specify which level of system message should be logged to the Syslog Host. This setting applies to all syslog facilities.

2. Enter or modify the following settings:

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

## HTTP Configuration

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

## HTTP Statistics

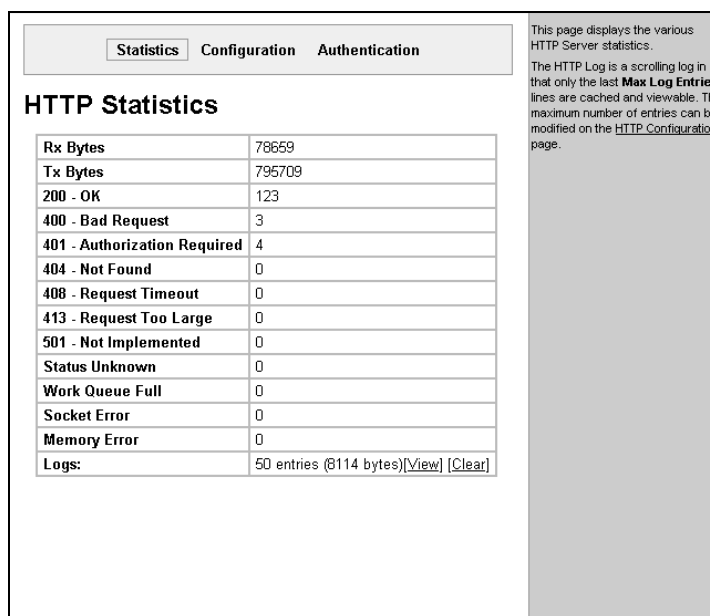
**Note:** The HTTP log is a scrolling log, with the last Max Log Entries cached and viewable. You can change the maximum number of entries that can be viewed on the HTTP Configuration Page.

### To view HTTP statistics:

This read-only page shows various statistics about the Hypertext Transfer Protocol (HTTP) server.

1. Click **HTTP** on the menu bar. The HTTP Statistics page displays.

Figure 8-7. HTTP Statistics



## HTTP Configuration

On this page you can change HTTP configuration settings.

### To configure HTTP:

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

Figure 8-8. HTTP Configuration

Statistics
**Configuration**
Authentication

## HTTP Configuration

HTTP Server: ☒ On ☐ Off  
 HTTP Port:   
 HTTPS Port:   
 HTTPS Protocols  
     SSL3: ☐ Enable ☐ Disable  
     TLS1.0: ☐ Enable ☐ Disable  
     TLS1.1: ☐ Enable ☐ Disable  
 Max Timeout:  seconds  
 Max Bytes:   
 Logging: ☐ On ☐ Off  
 Max Log Entries:   
 Log Format:

---

### Current Configuration

HTTP Status:	On (running)
HTTP Port:	80
HTTPS Port:	443
HTTPS Protocols:	SSL3, TLS1.0, TLS1.1
Max Timeout:	10seconds
Max Bytes:	40960
Logging:	On
Max Log Entries:	50
Log Format:	%h %t "%r" %s %B "%{Referer}i" "%{User-Agent}i"
Logs:	50 entries (7446 bytes) <a href="#">[View]</a> <a href="#">[Clear]</a>

Both the **HTTP Port** and **HTTPS Port** (SSL) can be overridden. The HTTP Server will only listen on the **HTTPS Port** when an **SSL Certificate** is configured for the device and at least one SSL protocol version is enabled in **HTTPS Protocols**.

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

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

**Log Format Directives**

%a	remote IP address (could be a proxy)
%b	bytes sent excluding headers
%B	bytes sent excluding headers (0 = "-")
%h	remote host (same as '%a')
%(h)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

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

## 2. Enter or modify the following settings:

HTTP Configuration Page Settings	Description
HTTP Server	Select <b>On</b> to enable the HTTP server.
HTTP Port	Enter the port for the HTTP server to use. The default is <b>80</b> .
HTTPS Port	Enter the port for the HTTPS server to use. The default is <b>443</b> . The HTTP server only listens on the <b>HTTPS Port</b> when an SSL certificate is configured.
HTTPS Protocols	Select to enable or disable the following protocols: <b>SSL3</b> = Secure Sockets Layer version 3  <b>TLS1.0</b> = Transport Layer Security version 1.0. TLS 1.0 is the successor of SSL3 as defined by the IETF.  <b>TLS1.1</b> = Transport Layer Security version 1.1  The protocols are enabled by default. A server certificate and associated private key need to be installed in the <b>SSL</b> configuration section to use <b>HTTPS</b> .



HTTP Configuration Page Settings	Description
<b>Max Timeout</b>	Enter the maximum time for the HTTP server to wait when receiving a request. This prevents Denial-of-Service (DoS) attacks. The default is <b>10</b> seconds.
<b>Max Bytes</b>	Enter the maximum number of bytes the HTTP server accepts when receiving a request. The default is <b>40</b> KB (this prevents DoS attacks).
<b>Logging</b>	Select <b>On</b> to enable HTTP server logging.
<b>Max Log Entries</b>	Sets the maximum number of HTTP server log entries. Only the last <b>Max Log Entries</b> are cached and viewable.
<b>Log Format</b>	Set the log format string for the HTTP server. Follow these <b>Log Format</b> rules: <b>%a</b> - remote IP address (could be a proxy) <b>%b</b> - bytes sent excluding headers <b>%B</b> - bytes sent excluding headers (0 = '-') <b>%h</b> - remote host (same as '%a') <b>%{h}i</b> - header contents from request (h = header string) <b>%m</b> - request method <b>%p</b> - ephemeral local port value used for request <b>%q</b> - query string (prepend with '?' or empty '-') <b>%t</b> - timestamp HH:MM:SS (same as Apache '%(%H:%M:%S)t' or '%(%T)t') <b>%u</b> - remote user (could be bogus for 401 status) <b>%U</b> - URL path info <b>%r</b> - first line of request (same as '%m %U%q <version>') <b>%s</b> - return status

- Click **Submit**. Changes are applied immediately to the MatchPort b/g Pro.

## HTTP Authentication

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

### To configure HTTP authentication settings:

- Click **HTTP** on the menu bar and then **Authentication** at the top of the page. The HTTP Authentication page opens.

Figure 8-9. HTTP Authentication

Statistics
Configuration
Authentication

## HTTP Authentication

URI:

Realm:

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

Username:

Password:

---

### Current Configuration

URI:	/ <a href="#">[Delete]</a>
Realm:	config
AuthType:	Digest
Users:	admin <a href="#">[Delete]</a>

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

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

**None**  
no authentication necessary

**Basic**  
encodes passwords using Base64

**Digest**  
encodes passwords using MD5

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

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

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

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

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

Multiple users can be configured within a single authentication directive.

2. Enter or modify the following settings:

HTTP Authentication Settings	Description
URI	Enter the Uniform Resource Identifier (URI).
Realm	Enter the domain, or realm, used for HTTP. Required with the URI field.
Auth Type	<p>Select the authentication type:  <b>None</b> = no authentication is necessary.</p> <p><b>Basic</b> = encodes passwords using Base64.</p> <p><b>Digest</b> = encodes passwords using MD5.</p> <p><b>SSL</b> = the page can only be accessed over SSL (no password is required).</p> <p><b>SSL/Basic</b> = the page is accessible only over SSL and encodes passwords using Base64.</p> <p><b>SSL/Digest</b> = the page is accessible only over SSL and encodes passwords using MD5.</p>
Username	Enter the <b>Username</b> used to access the URI.
Password	Enter the <b>Password</b> for the <b>Username</b> .

3. In the **Current Configuration** table, delete and clear currently stored settings as necessary.
4. Click **Submit**. Changes are applied immediately to the MatchPort b/g Pro.

**Notes:**

- ◆ More than one **Username** per **URI** is permitted. Click **Submit** and enter the next **Username** as necessary.
- ◆ The **URI**, **realm**, **username**, and **password** are user-specified, free-form fields. The **URI** must match the directory created on the MatchPort 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 are also stored to the file system's `cfg_log.txt` file.

**To configure RSS settings:**

1. Click **RSS** on the menu bar. The RSS page opens and displays the current RSS configuration.

**Figure 8-10. RSS**

### RSS

RSS Feed: ☐ On ☒ Off

Persistent: ☐ On ☒ Off

Max Entries:

### Current Configuration

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

An RDF Site Summary (RSS) syndication feed is served by the HTTP Server. This feed contains up-to-date information regarding the configuration changes that occur on the device.

Specifying the RSS Feed to be **Persistent** results in the data being stored on the filesystem. The file used is `/cfg_log.txt`. This allows feed data to be available across reboots (or until the factory defaults are set).

Each RSS Feed entry is prefixed with a timestamp as follows: "[BC: HH: MM: SS]". "BC" is the Boot Cycle value. This value is the number of times the device has been rebooted since the factory defaults were last loaded. The resulting "HH: MM: SS" is the time since the device booted up. This somewhat cryptic scheme is used because no Real Time Clock is available.

The RSS Feed is a scrolling feed in that only the last **Max Entries** entries are cached and viewable.

Simply register the **RSS Feed** within your favorite RSS aggregator and you will automatically be notified of any configuration changes that occur.

2. Enter or modify the following settings:

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

3. In the **Current Configuration** table, view and clear currently stored settings as necessary.
4. Click **Submit**. Changes are applied immediately to the MatchPort b/g Pro.

## LPD Settings

In addition to its other functions, the MatchPort b/g Pro acts as a print server if a printer is connected to one of its serial ports.

Clicking the **LPD** (Line Printer Daemon) link in the menu bar displays the LPD Statistics page. This page has three links at the top 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 Page

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

#### To view LDP statistics:

1. Click **LDP** on the menu bar. The LDP page displays LDP statistics.

Figure 8-11. LDP Statistics

LPD 1 LPD 2

[Statistics](#)
[Configuration](#)
[Print Test Page](#)

### LPD 1- Statistics

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

This page displays various statistics and current usage information of the LPD subsystem.

When a document is printed, the remote client information is displayed as well as the number of print jobs printed since boot up, and the total number of bytes printed.

If a client is printing, a **Kill** link is displayed next to the client information. The **Kill** link will force the LPD server to kill (abort) any current, active print jobs.

## LPD Configuration Page

Here you can change LPD configuration settings.

### To configure LPD settings:

1. Click **LPD** on the menu bar, select the LPD line and click **Configuration**. The LPD Configuration page displays.

Figure 8-12. LPD Configuration

LPD Configuration Page Settings	Description
Banner	Select <b>Enabled</b> to print the banner even if the print job does not specify to do so. Selected by default.
Binary	Select <b>Enabled</b> for the MatchPort b/g Pro is to pass the entire file to the printer unchanged. Otherwise, the MatchPort b/g Pro 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. Unselected by default.
Start of Job	Select <b>Enabled</b> to print a "start of job" string before sending the print data.
End of Job	Select <b>Enabled</b> to send an "end of job" string.
Formfeed	Select <b>Enabled</b> to force the printer to advance to the next page at the end of each print job.
Convert Newlines	Select <b>Enabled</b> to convert single newlines and carriage returns to DOS-style line endings.
SOJ String	<p>If <b>Start of Job</b> (above) is enabled, enter the string to be sent to the printer at the beginning of a print job. The limit is 100 characters.</p> <p>Indicate whether the string is in text or binary format.</p>
EOJ String	<p>If <b>End of Job</b> (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.</p>
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 defaults are <b>LPDQueue1 (port 1)</b> <b>LPDQueue2 (port 2)</b> .

## 9: Security Settings

### SSH Settings

Secure Shell (SSH) is a protocol used to access a remote computer over an encrypted channel. It is a protocol for managing the security of data transmission over the Internet. It provides encryption, authentication, and message integrity services. This page has four links at the top for viewing and changing SSH server host keys, SSH server authorized keys, SSH client known hosts, and SSH client users.

**Note:** For more information, see [Security in Detail](#) on page 145.

#### SSH Server's Host Keys

To configure the SSH server's host keys:

1. Click **SSH** on the menu bar. The SSH Server: Host Keys page displays.

Figure 9-1. SSH Server: Host Keys

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

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

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

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

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

2. Enter or modify the following settings:

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

- Click **Submit**. Changes are applied immediately to the MatchPort b/g Pro.

## SSH Server's Authorized Users

On this page you can change SSH server settings for authorized users.

SSH Server Authorized Users are accounts on the MatchPort that can be used to log into the MatchPort b/g Pro 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. Click **SSH** on the menu bar and then **Server Authorized Users** at the top of the page. The SSH Server: Authorized Users page displays.

**Figure 9-2. SSH Server: Authorized Users**

2. Enter or modify the following settings:

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

3. Click **Submit**. Changes are applied immediately to the MatchPort b/g Pro.



## 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. Click **SSH** on the menu bar and then **Client Known Hosts** at the top of the page. The SSH Client: Known Hosts page displays.

Figure 9-3. SSH Client: Known Hosts

2. Enter or modify the following settings:

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

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

3. In the **Current Configuration** table, delete currently stored settings as necessary.
4. Click **Submit**. Changes are applied immediately to the MatchPort b/g Pro.

## SSH Client User Configuration

On this page you can change SSH client settings for users.

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

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

### To configure the SSH client's users:

1. Click **SSH** on the menu bar and then **SSH Client Users** at the top of the page. The SSH Client: Users page displays.

Figure 9-4. SSH Client: Users

SSH Server: Host Keys
SSH Client: Known Hosts

SSH Server: Authorized Users
SSH Client: Users

### SSH Client: Users

Username:

Password:

Remote Command:

Private Key:

Public Key:

Key Type: ☒ RSA ☐ DSA

#### Create New Keys

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

Username:

Key Type: ☒ RSA ☐ DSA

Bit Size: ☒ 512 ☐ 768 ☐ 1024

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

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

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

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

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

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

---

#### Current Configuration

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

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

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

2. Enter or modify the following settings:

SSH Client: Users Page Settings	Description
Username	Enter the name that the MatchPort b/g Pro uses to connect to the SSH client user.
Password	Enter the password associated with the username.
Remote Command	Enter the command that can be executed remotely. Default is <b>shell</b> , which tells the SSH server to execute a remote shell upon connection. This command can be changed to anything the remote host can perform.
Private Key	Enter the name of the existing private key you want to use with this SSH client user. You can either enter the path and name of the key, or use the <b>Browse</b> button to

SSH Client: Users Page Settings	Description
	select the key.
Public Key	Enter the path and name of the existing public key you want to use with this SSH client user or use the <b>Browse</b> button to select the key.
Key Type	Select the key type to be used. Choices are:  <b>RSA</b> = use this key with the SSH1 and SSH2 protocols. <b>DSA</b> = use this key with the SSH2 protocol.
<b>Create New Keys</b>	
Username	Enter the name of the user associated with the new key.
Key Type	Select the key type to be used for the new key. Choices are:  <b>RSA</b> = use this key with the SSH1 and SSH2 protocols. <b>DSA</b> = use this key with the SSH2 protocol.
Bit Size	Select the bit length of the new key:  <b>512</b> <b>768</b> <b>1024</b>  Using a larger Bit Size takes more time to generate the key. Approximate times are: 10 seconds for a 512 bit RSA Key 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  Some SSH clients require RSA host keys to be at least 1024 bits long.

3. Click **Submit**. Changes are applied immediately to the MatchPort b/g Pro.
4. In the **Current Configuration** table, delete currently stored settings as necessary.
5. Click **Submit**. Changes are applied immediately to the MatchPort b/g Pro.

## SSL Settings

Secure Socket 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. On the MatchPort b/g Pro, it is also used as the basis for several of the **EAP** security protocols for **WPA** and **WPA2**.

Certificate/Private key combinations can be obtained from an external Certificate Authority (CA) and downloaded into the unit, or 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 [14: Security in Detail](#).

**To configure the MatchPort b/g Pro's SSL settings:**

1. Click **SSL** from the main menu. The SSL page displays.

**Figure 9-5. SSL**

## SSL

### Upload Certificate

New Certificate:

New Private Key:

### Upload Authority Certificate

Authority:

### Create New Self-Signed Certificate

Country (2 Letter Code):

State/Province:

Locality (City):

Organization:

Organization Unit:

Common Name:

Expires:  mm/dd/yyyy

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

Type: ☐ RSA ☐ DSA

### Current SSL Certificates

None configured

### Current Certificate Authorities

None configured

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

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

**WARNING:** When generating a new self-signed SSL Certificate, using a large key size can result in a VERY LONG key generation time. Tests on this hardware have shown it can take upwards of:

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 minutes for a 1024 bit DSA Key

SSL Page Settings	Description
<b>Upload Certificate</b>	
New Certificate	<p>This certificate identifies the MatchPort b/g Pro to peers. It is used for HTTPS, SSL Tunneling, and EAP-TLS.</p> <p>Enter the path and name of the certificate you want to upload, or use the <b>Browse</b> button to select the certificate.</p> <p><b>RSA</b> or <b>DSA</b> certificates with 512 to 1024 bit public keys are allowed.</p> <p>The format of the file must be <b>PEM</b>. The file must start with "-----"</p>

SSL Page Settings	Description
	BEGIN CERTIFICATE-----" and end with "-----END CERTIFICATE-----". Some Certificate Authorities add comments before and/or after these lines. Those need to be deleted before upload.
New Private Key	<p>Enter the path and name of the private key you want to upload, or use the <b>Browse</b> 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 <b>PEM</b>. The file must start with "-----BEGIN RSA PRIVATE KEY-----" and end with "-----END RSA PRIVATE KEY-----". Read <b>DSA</b> instead of <b>RSA</b> in case of a <b>DSA</b> key. Some Certificate Authorities add comments before and/or after these lines. Those need to be deleted before upload.</p>
<b>Upload Authority Certificate</b>	
Authority:	<p>One or more authority certificates are needed to verify a peer's identity. It is used for SSL Tunneling and EAP-TLS, EAP-TTLS, PEAP. 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 <b>Browse</b> button to select the certificate.</p> <p><b>RSA</b> or <b>DSA</b> certificates with 512 to 1024 bit public keys are allowed.</p> <p>The format of the file must be <b>PEM</b>. 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>
<b>Create New Self-Signed Certificate</b>	
Country (2 Letter Code)	<p>Enter the 2-letter country code to be assigned to the new self-signed certificate.</p> <p><b>Examples:</b> 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><b>Example:</b> If your company is called Widgets, and you are setting up a web server for the Sales department, enter Widgets for the organization.</p>
Organization Unit	<p>Enter the organizational unit to be associated with the new self-signed certificate.</p> <p><b>Example:</b> If your company is setting up a web server for the Sales department, enter Sales for your organizational unit.</p>
Common Name	Enter the same name that the user will enter when requesting

SSL Page Settings	Description
	<p>your web site.</p> <p><b>Example:</b> If a user enters <code>http://www.widgets.abccompany.com</code> to access your web site, the <b>Common Name</b> would be <code>www.widgets.abccompany.com</code>.</p>
Expires	<p>Enter the expiration date, in mm/dd/yyyy format, for the new self-signed certificate.</p> <p><b>Example:</b> An expiration date of May 9, 2007 is entered as <code>05/09/2007</code>.</p>
Key length	<p>Select the bit size of the new self-signed certificate. Choices are:</p> <p><b>512 bits</b></p> <p><b>768 bits</b></p> <p><b>1024 bits</b></p> <p>The larger the bit size, the longer it takes to generate the key. Approximate times are:</p> <p>10 seconds for a 512-bit RSA key</p> <p>15 seconds for a 768-bit RSA key</p> <p>1 minute for a 1024-bit RSA key</p> <p>30 seconds for a 512-bit DSA key</p> <p>2 minutes for a 768-bit DSA key</p> <p>6 minute for a 1024-bit DSA key</p>
Type	<p>Select the type of key:</p> <p><b>RSA</b> = Public-Key Cryptography algorithm based on large prime numbers, invented by Rivest Shamir and Adleman. Used for encryption and signing.</p> <p><b>DSA</b> = 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.</p>

## 10: Maintenance and Diagnostics Settings

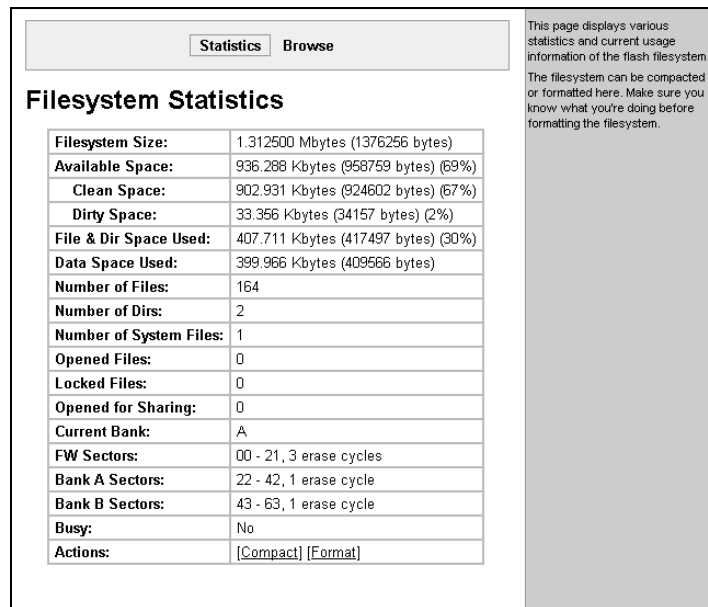
### Filesystem Configuration

The MatchPort b/g Pro uses a flash filesystem to store files. Use the Filesystem option to view current file diagnostics or modify files.

### Filesystem Statistics

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

Figure 10-1. Filesystem Statistics





**To view filesystem statistics, compact, or format the MatchPort b/g Pro's filesystem:**

1. Click **Filesystem** on the menu bar. The Filesystem page opens and displays the current filesystem statistics and usage.
2. To compact the files, click **Compact**.

***Note:** Data can be lost if power is cycled when compacting the filesystem.*

3. To reformat the filesystem, click **Format**.

***Note:** All files and configuration settings on the filesystem are destroyed upon formatting, including Web Manager files. Back up all files as necessary. Upon formatting, the current configuration is lost.*

**Filesystem Browser****To browse the MatchPort b/g Pro's filesystem:**

1. Click **Filesystem** on the menu bar and then **Browse** at the top of the page. The Filesystem Browser page opens and displays the current filesystem configuration.

Figure 10-2. Filesystem Browser

Statistics
Browse

## Filesystem Browser

/
 

X http

---

**Create**

File:  Create

Directory:  Create

---

**Upload File**

Browse...

Upload

---

**Copy File**

Source:

Destination:

Copy

---

**Move**

Source:

Destination:

Move

---

**TFTP**

Action: ☐ Get ☐ Put

Mode: ☐ ASCII ☐ Binary

Local File:

Remote File:

Host:

Port:

Transfer

From here you can browse and manipulate the entire filesystem. Directories can be created, deleted, moved, and renamed. A directory must be empty before it can be deleted.

Files can be created, deleted, moved, renamed, uploaded via HTTP, and transferred to and from a TFTP server. Newly created files will be empty.

2. Click 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, click the folder or directory and then enter the parameters in the settings listed below.

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

## Protocol Stack Configuration

To configure the MatchPort b/g Pro's network stack protocols:

1. Click **Protocol Stack** on the menu bar. The Protocol Stack page displays the settings for TCP, ICMP, ARP, and ARP Cache and the status.

Figure 10-3. Protocol Stack

### TCP

Send RSTs: ☐ On ☒ Off

#### Current State

Send RSTs:	On
Total Out RSTs:	5
Total In RSTs:	0

### ICMP

Enable: ☐ On ☒ Off

#### Current State

Enable:

### ARP

ARP Timeout:  seconds

#### Current State

ARP Timeout:

### ARP Cache

IP Address:

MAC Address:

#### Current State

Address	Age	MAC Address	Type	Interface
172.20.197.254 <input type="button" value="Remove"/>	0.4	00:d0:04:02:c0:00	Dynamic	1

This page contains lower level Network Stack specific configuration items.

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

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

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

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

- Enter or modify the following settings:

Protocol Stack Page Settings	Description
<b>TCP</b>	
<b>Send RSTs</b>	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. Sending this flag may pose a security risk. Select <b>Off</b> to disable the sending of the RST flag.
<b>ICMP</b>	
<b>Enable</b>	Internet Control Message Protocol (ICMP) can be used as an error-reporting protocol between two hosts. Commands such as <code>ping</code> use this protocol. Sending and processing ICMP messages may pose a security risk.
<b>ARP</b>	
<b>ARP Timeout</b>	Enter the time, in milliseconds, for the ARP timeout. This is the maximum duration an address remains in the cache.
<b>ARP Cache</b>	
<b>IP Address</b>	Enter the IP address to add to the ARP table.
<b>MAC Address</b>	Enter the MAC address to add to the ARP table.
<i><b>Note:</b> Both the IP and MAC addresses are required for the ARP cache.</i>	
<b>Current State</b>	
<b>Clear</b>	Select <b>Clear</b> to remove all entries in the ARP table.
<b>Remove</b>	Removes a specific entry from the ARP table.

- Click **Submit** after each modified field. Changes are applied immediately to the MatchPort b/g Pro.

## IP Address Filter

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

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

### To configure the IP address filter:

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

Figure 10-4. IP Address Filter Configuration

### IP Address Filter

IP Address:

Network Mask:

The IP Address Filter table contains all the IP Addresses and Subnets that **ARE ALLOWED** to send data to this device. All packets from IP Addresses not in this list are ignored and thrown away.

If the filter list is empty then all IP Address are allowed.

WARNING: If using DHCP/BOOTP, make sure the IP Address of the DHCP/BOOTP server is in the filter list.

---

### Current State

The IP Filter Table is empty so ALL addresses are allowed.

- Enter or modify the following settings:

IP Address Filter Page 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.

- In the **Current State** table, click **Remove** to delete settings as necessary.
- Click **Submit**. Changes are applied immediately to the MatchPort b/g Pro.

## 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 17.

### To configure the query port server:

- Click **Query Port** on the menu bar. The Query Port page opens to display the current configuration.

Figure 10-5. Query Port Configuration

## Query Port

Query Port Server: ☒ On ☐ Off

---

### Current Configuration and Statistics

Query Port Status:	On (running)
In Valid Queries:	1
In Unknown Queries:	0
In Erroneous Packets:	0
Out Query Replies:	1
Out Errors:	0
Last Connection:	172.19.100.233:32770

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

2. Select **On** to enable the query port server.
3. Click **Submit**. Changes are applied immediately to the MatchPort b/g Pro.

## Diagnostics

The MatchPort b/g Pro has several tools for diagnostics and statistics. The options at the top of the page allow for the configuration or viewing of MIB2 statistics, IP socket information, ping, traceroute, DNS lookup, memory, buffer pools, processes, and hardware.

### Hardware

This read-only page displays the current hardware configuration.

#### To display the MatchPort b/g Pro's hardware diagnostics:

1. Click **Diagnostics** on the menu bar. The Diagnostics: Hardware page opens and displays the current hardware configuration.

Figure 10-6. Diagnostics: Hardware

Hardware

MIB-II

IP Sockets

This page shows the basic hardware information for the device.

Ping

Traceroute

DNS Lookup

Memory

Buffer Pools

Processes

## Diagnostics: Hardware

### Current Configuration

CPU Type:	MCF5208
CPU Speed:	83.333000 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:	4.000000 Mbytes (4194304 bytes)
Flash Sector Size:	64.000 Kbytes (65536 bytes)
Flash Sector Count:	64
Flash ID:	0x20

## MIB-II Statistics

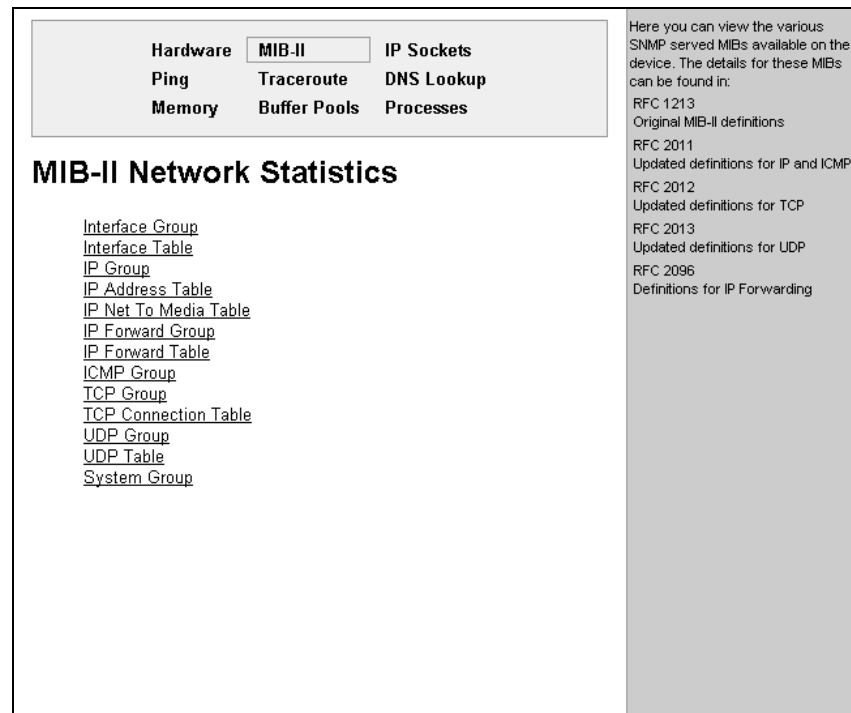
The MIB-II Network Statistics page displays the various SNMP-served Management Information Bases (MIBs) available on the MatchPort b/g Pro.

### To view MatchPort b/g Pro's MIB-II statistics:

1. Click **Diagnostics** on the menu bar and then **MIB-II Statistics** at the top of the page menu. The MIB2 Network Statistics page opens.



Figure 10-7. MIB-II Network Statistics



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

### MIB-II Network Statistics

[Interface Group](#)  
[Interface Table](#)  
[IP Group](#)  
[IP Address Table](#)  
[IP Net To Media Table](#)  
[IP Forward Group](#)  
[IP Forward Table](#)  
[ICMP Group](#)  
[TCP Group](#)  
[TCP Connection Table](#)  
[UDP Group](#)  
[UDP Table](#)  
[System Group](#)

Here you can view the various SNMP served MIBs available on the device. The details for these MIBs can be found in:

- 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

- Click any of the available links to open the corresponding table and statistics. For more information, refer to the following Requests for Comments (RFCs):

<b>RFC 1213</b>	Original MIB2 definitions.
<b>RFC 2011</b>	Updated definitions for IP and ICMP.
<b>RFC 2012</b>	Updated definitions for TCP.
<b>RFC 2013</b>	Updated definitions for UDP.
<b>RFC 2096</b>	Definitions for IP forwarding.

## IP Sockets

To display open network sockets on the MatchPort b/g Pro:

- Click **Diagnostics** on the menu bar and then **IP Sockets** at the top of the page. The IP Sockets page opens and displays all of the open network sockets on the MatchPort b/g Pro.

Figure 10-8. IP Sockets

**Hardware**  
Ping  
Memory

**MIB-II**  
Traceroute  
Buffer Pools

IP Sockets

  
DNS Lookup  
Processes

### IP Sockets

Protocol	RxQ	TxQ	LocalAddr:Port	RemoteAddr:Port	State
UDP	0	0	172.20.197.60:161	255.255.255.255:0	
TCP	0	8	172.20.197.60:80	172.18.100.26:1306	ESTABLISHED
TCP	0	0	172.20.197.60:21	255.255.255.255:0	LISTEN
UDP	0	0	172.20.197.60:69	255.255.255.255:0	
TCP	0	0	172.20.197.60:80	255.255.255.255:0	LISTEN
UDP	0	0	172.20.197.60:30718	172.20.197.46:26672	ESTABLISHED
TCP	0	0	172.20.197.60:23	255.255.255.255:0	LISTEN
TCP	0	0	172.20.197.60:22	255.255.255.255:0	LISTEN
TCP	0	0	172.20.197.60:10001	255.255.255.255:0	LISTEN
TCP	0	0	172.20.197.60:10002	255.255.255.255:0	LISTEN

This page lists all the currently open network sockets on the device.

## Ping

To ping a remote device or computer:

1. Click **Diagnostics** on the menu bar and then **Ping** at the top of the page. The Diagnostics: Ping page opens.

Figure 10-9. Diagnostics: Ping

2. Enter or modify the following settings:

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

1. Click **Diagnostics** on the menu bar and then **Traceroute** at the top of the page. The Diagnostics: Traceroute page opens.

Figure 10-10. Diagnostics: Traceroute

Hardware

Ping

Memory

MIB-II

**Traceroute**

Buffer Pools

IP Sockets

DNS Lookup

Processes

Specify either a DNS Hostname or IP Address when performing a traceroute to a network host.

### Diagnostics: Traceroute

Host:

#### TracerouteResults

1	172.19.0.1	1 ms
2	67.134.254.1	2 ms
3	67.134.135.149	4 ms
4	205.171.13.13	4 ms
5	67.14.12.58	12 ms
6	205.171.214.38	13 ms
7	207.45.213.133	13 ms
8	207.45.213.130	14 ms
9	216.115.106.177	15 ms
10	66.218.82.219	14 ms
11	66.94.234.13	13 ms

2. Enter or modify the following setting:

Diagnostics: Traceroute Page Settings	Description
Host	Enter the IP address or DNS hostname. This address is used to show the path between it and the MatchPort b/g Pro when issuing the traceroute command.

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

## DNS Lookup

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

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

### To use forward or reverse DNS lookup:

1. Click **Diagnostics** on the menu bar and then **DNS Lookup** at the top of the page. The Diagnostics: DNS Lookup page opens.

Figure 10-11. Diagnostics: DNS Lookup

2. Enter or modify the following field:

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

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

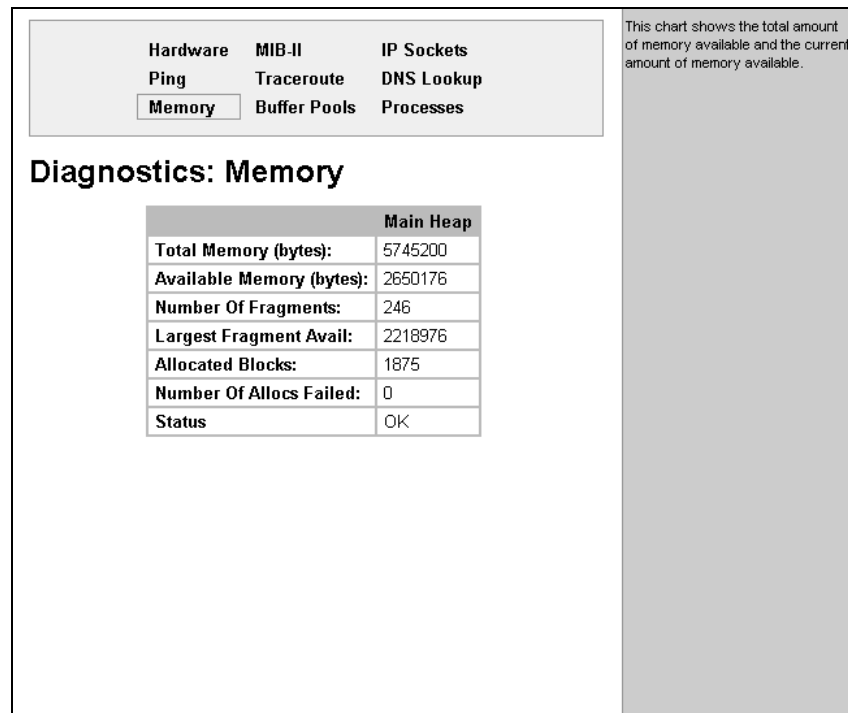
## Memory

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

### To display memory statistics for the MatchPort b/g Pro:

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

Figure 10-12. Diagnostics: Memory



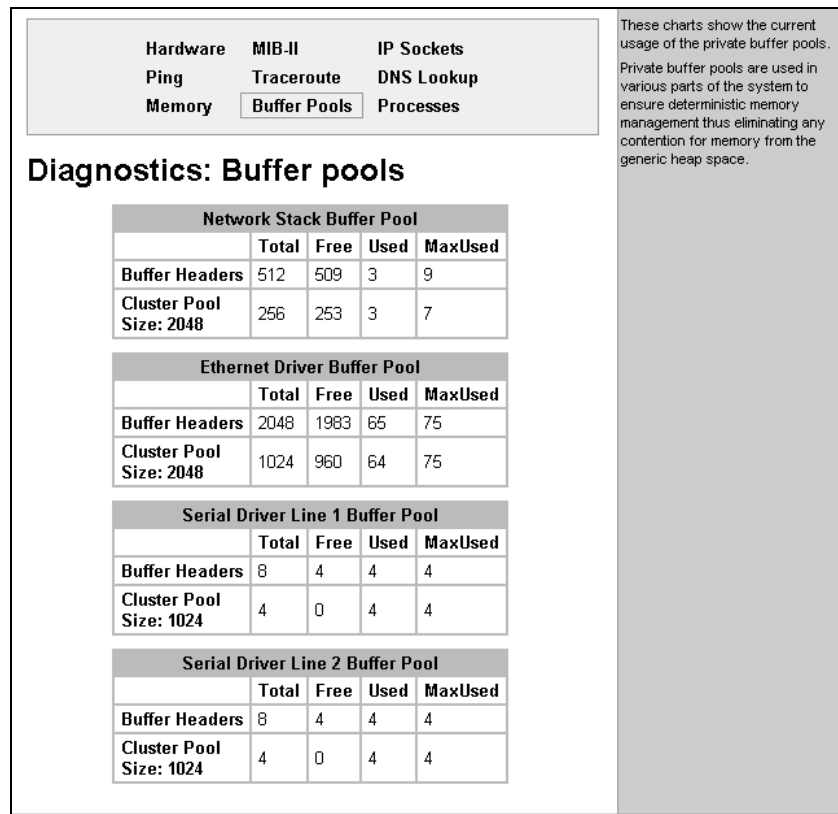
## Buffer Pools

Several parts of the MatchPort b/g Pro system use private buffer pools to ensure deterministic memory management.

### To display the MatchPort b/g Pro's buffer pools:

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

Figure 10-13. Diagnostics: Buffer Pools



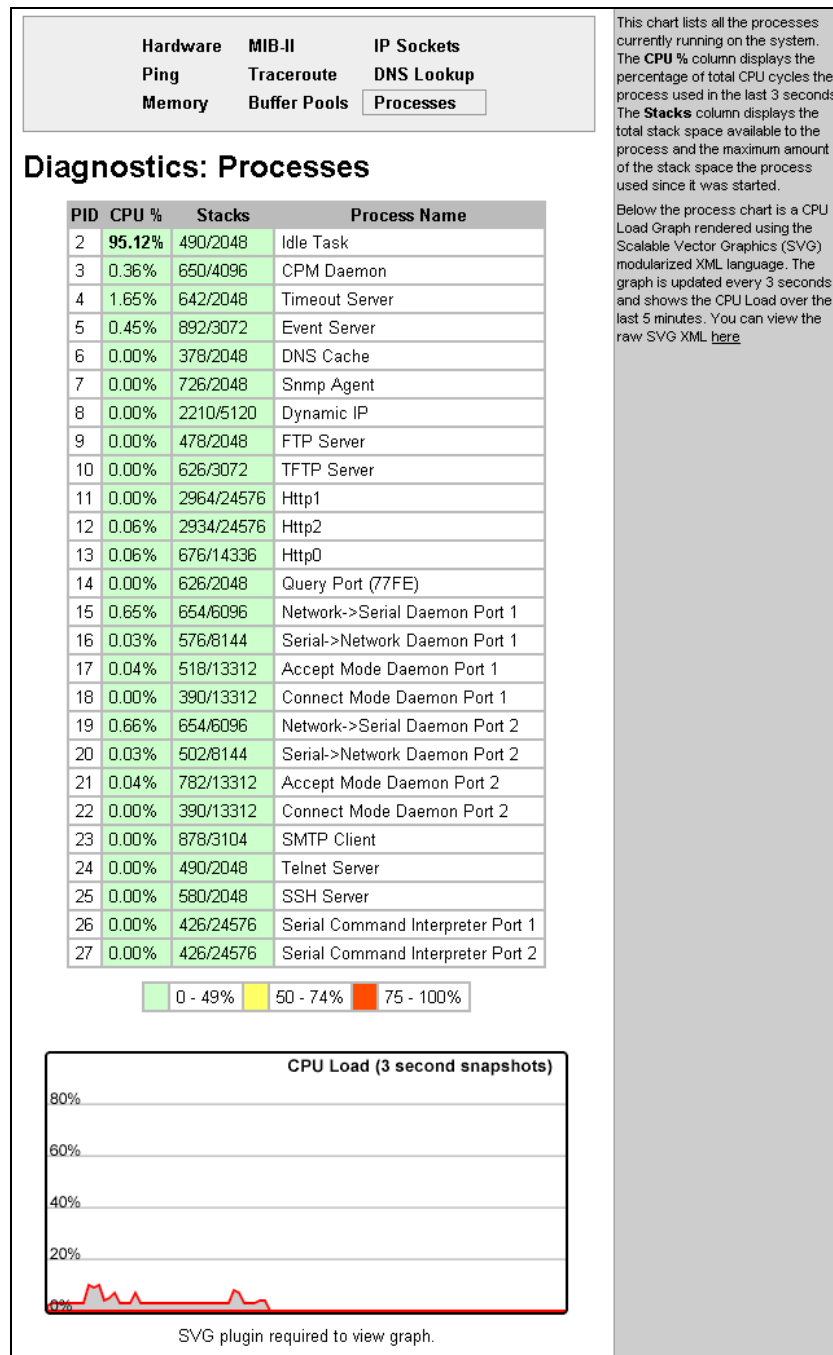
## Processes

The MatchPort b/g Pro Processes page displays all the processes currently running on the system. It displays 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 on the MatchPort b/g Pro and their associated statistics:**

1. Click **Diagnostics** on the menu bar and then **Processes** at the top of the page. The Diagnostics: Processes page opens.

Figure 10-14. Diagnostics: Processes



This chart lists all the processes currently running on the system. The **CPU %** column displays the percentage of total CPU cycles the process used in the last 3 seconds. The **Stacks** column displays the total stack space available to the process and the maximum amount of the stack space the process used since it was started.

Below the process chart is a CPU Load Graph rendered using the Scalable Vector Graphics (SVG) modularized XML language. The graph is updated every 3 seconds and shows the CPU Load over the last 5 minutes. You can view the raw SVG XML [here](#).

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



## CPU Power Management

The CPU Power Management page allows you to enable the MatchPort b/g Pro to turn off the CPU automatically when it is idling. This saves in the power consumption when the device server is not 100 percent engaged. Start up latency is insignificant.

**Note:** This is different from WLAN Power Management.

Figure 10-15. CPU Power Management

CPU Power Management	
State:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled

This page allows configuration of the CPU Power Management feature. CPU Power Management controls the power management of the CPU, its on-chip peripherals, and external memory.

Note: This is different from WLAN Power Management.

To configure the power management feature:

1. Click **CPU Power Mgmt** on the menu bar. The Power Management page opens.
2. Select whether the **State** of the power management should be enabled or disabled. The default is **Enabled**.
3. Click **Submit**.

## System Configuration

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

Figure 10-16. System

## System

---

### Reboot Device

---

### Restore Factory Defaults

---

### Upload New Firmware

---

### Name

Short Name:

Long Name:

---

### Current Configuration

Firmware Version:	1.0.0.1R1
Short Name:	matchport
Long Name:	Lantronix MatchPort AR

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

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

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

**To configure the MatchPort b/g Pro's system settings:**

1. Click **System** on the menu bar. The System page opens.
2. Configure the following settings:

System Page Settings	Description
<b>Reboot Device</b>	Click <b>Reboot</b> to reboot the MatchPort b/g Pro. The system refreshes and redirects the browser to the MatchPort b/g Pro's home page.
<b>Restore Factory Defaults</b>	Click <b>Factory Defaults</b> to restore the MatchPort b/g Pro to the original factory settings. All configurations will be lost. The MatchPort b/g Pro automatically reboots upon setting back to the defaults.
<b>Upload New Firmware</b>	Click <b>Browse</b> to locate the firmware file location. Click <b>Upload</b> to install the firmware on the MatchPort b/g Pro. The device automatically reboots upon the installation of new firmware.
<b>Name</b>	Enter a new <b>Short Name</b> and a <b>Long Name</b> (if necessary). The <b>Short Name</b> maximum is 32 characters. The <b>Long Name</b> maximum is 64 characters. Changes take place upon the next reboot.

# 11: Advanced Settings

## Email Configuration

The MatchPort b/g Pro allows you to view and configure four email alerts relating to the Configuration Pins (CPs).

**Note:** The following section describes the steps to configure **Email 1**; these steps also apply to **Email 2**, **Email 3**, and **Email 4** menu options.

### Email Statistics

This read-only page shows various statistics and current usage information about the email subsystem.

1. Click **Email 1** at the top of the page to view its statistics.

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

Figure 11-1. Email Statistics

<div>Email 1   Email 2   Email 3   Email 4</div> <div>Statistics   Configuration   Send Email</div>		<p>This page displays various statistics and current usage information of the Email subsystem.</p> <p>When transmitting an Email message the entire conversation with the SMTP server is logged and displayed here. This is a scrolling log in that only the last 100 lines are cached and viewable.</p>						
<h3>Email 1- Statistics</h3>								
<table border="1"><tr><td>Sent successfully (w/retries):</td><td>0 / 0</td></tr><tr><td>Not sent due to excessive errors:</td><td>0</td></tr><tr><td>In transmission queue:</td><td>0</td></tr></table>			Sent successfully (w/retries):	0 / 0	Not sent due to excessive errors:	0	In transmission queue:	0
Sent successfully (w/retries):	0 / 0							
Not sent due to excessive errors:	0							
In transmission queue:	0							
<div><b>Log [Clear]</b></div> <p>No log data available.</p>								

## Email Configuration

To configure MatchPort b/g Pro's email settings:

1. Click **Email** on the menu bar and then **Configuration** at the top of the page. The Email Configuration page opens to display the current Email configuration.

Figure 11-2. Email Configuration

The screenshot shows the 'Email Configuration' page. At the top, there are tabs for 'Email 1', 'Email 2', 'Email 3', and 'Email 4'. Below these are buttons for 'Statistics', 'Configuration' (which is selected), and 'Send Email'. The main heading is 'Email 1- Configuration'. Below this, there are input fields for 'To:', 'Cc:', 'From:', 'Reply-To:', 'Subject:', 'File:', and 'Overriding Domain:'. There are also input fields for 'Server Port:' and 'Local Port:', with a note 'or Random' next to the Local Port field. A 'Priority:' section has radio buttons for 'Urgent', 'High', 'Normal' (which is selected), 'Low', and 'VeryLow'. Below this is a 'Trigger Email Send:' section with a 'CP Group:' input field and a 'Value:' input field. A 'Submit' button is at the bottom left of the configuration area. Below the configuration area is a section titled 'Current Configuration' which contains a table showing the current settings.

Current Configuration	
To:	<None>
Cc:	<None>
From:	<None>
Reply-To:	<None>
Subject:	<None>
File:	<None>
Overriding Domain:	<None>
Server Port:	25
Local Port:	Random
Priority:	Normal
Trigger Email Send:	Disabled

2. Enter or modify the following settings:

Email – Configuration Page Settings	Description
To	Enter the email address to which the email alerts will be sent.
CC	Enter the email address to which the email alerts will be

Email – Configuration Page Settings	Description
	copied.
<b>From</b>	Enter the email address to list in the From field of the email alert.
<b>Reply-To</b>	Enter the email address to list in the Reply-To field of the email alert.
<b>Subject</b>	Enter the subject for the email alert.
<b>File</b>	Enter the path of the file to send with the email alert. This file displays within the message body of the email.
<b>Overriding Domain</b>	Enter the domain name to override the current domain name in EHLO (Extended Hello).
<b>Server Port</b>	Enter the SMTP server port number. The default is port <b>25</b> .
<b>Local Port</b>	Enter the local port to use for email alerts. The default is a random port number.
<b>Priority</b>	Select the priority level for the email alert.
<b>Trigger Email Send</b>	Configure this field to send an email based on a CP Group trigger. The MatchPort b/g Pro sends an email when the specified <b>Value</b> matches the current <b>Group's</b> value.

3. In the **Current Configuration** table, delete currently stored settings as necessary.
4. Click **Submit**. Changes are applied immediately to the MatchPort b/g Pro.

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

## Command Line Interface Settings

The Command Line Interface pages enable you to view statistics about the CLI servers listening on the Telnet and SSH ports and to configure CLI settings.

### Command Line Interface 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 remote client information displays.
- ◆ The number of bytes that have been sent and received displays.
- ◆ A **Kill** link (visible when a connection is active) can be used to terminate the connection.

1. Click **CLI** on the menu bar. The Command Line Interface Statistics page displays.

Figure 11-3. Command Line Interface Statistics

Statistics
Configuration

### Command Line Interface Statistics

Telnet Status	
Server Status:	Enabled (Waiting)
Local Port:	23
Last Connection:	<None>
Uptime:	1 days 17:50:25
Total Bytes In:	0
Total Bytes Out:	0
Current Connections:	<None>
SSH Status	
Server Status:	Enabled (Waiting)
Local Port:	22
Last Connection:	<None>
Uptime:	1 days 17:50:25
Total Bytes In:	0
Total Bytes Out:	0
Current Connections:	<None>

This page displays the current connection status of the CLI servers listening on the Telnet and SSH ports.

When a connection is active, the remote client information is displayed as well as the number of bytes that have been sent and received. Additionally, a **Clear** link will be present which can be used to kill the connection.

## CLI Configuration

On this page you can change CLI configuration settings.

### To configure the CLI:

1. Click **CLI** on the menu and then **Configuration** at the top of the page. The Command Line Interface Configuration page displays.

Figure 11-4. Command Line Interface Configuration

Statistics
Configuration

## Command Line Interface Configuration

Telnet Access: ☒ On ☐ Off

Telnet Port:

Telnet Max Sessions:

SSH Access: ☒ On ☐ Off

SSH Port:

SSH Max Sessions:

Login Password:

Enable Level Password:

Quit Connect Line:

Both the **Telnet Port** and **SSH Port** used by the CLI servers can be overridden.

The **Telnet Max Sessions** and **SSH Max Sessions** specify the maximum number of Telnet and SSH sessions that will be allowed. Each Telnet or SSH session requires 27 kbytes of Heap Memory.

The **Login Password** is used for initial login access from the Telnet port, SSH port, or any serial Line.

For the SSH server, the SSH Server Authorized Users are used for initial login access. [SSH](#)

The **Enable Level Password** is used for access to the 'enable' level within the CLI.

The **Quit Connect Line** string is used to terminate a connect line session and resume the CLI. Type <control> before any key to be pressed while holding down the Ctrl key, for example, <control>L.

---

### Current Configuration

Telnet Access:	Enabled
Telnet Port:	23
Telnet Max Sessions:	3
SSH Access:	Enabled
SSH Port:	22
SSH Max Sessions:	3
Login Password:	<None>
Enable Level Password:	<None>
Quit Connect Line:	<control>L

2. Enter or modify the following settings:

Command Line Interface Configuration Settings	Description
<b>Telnet Access</b>	Select <b>On</b> to enable Telnet access. Telnet is enabled by default.
<b>Telnet Port</b>	Enter the Telnet port to use for Telnet access. The default is <b>23</b> .
<b>Telnet Max Sessions</b>	Maximum number of simultaneous Telnet sessions.
<b>SSH Access</b>	Select <b>On</b> to enable SSH access. SSH is enabled by default.
<b>SSH Port</b>	Enter the SSH port to use for SSH access. The default is <b>22</b> .
<b>SSH Max Sessions</b>	Maximum number of simultaneous SSH sessions.
<b>Login Password</b>	Enter the password for Telnet access.
<b>Enable Level Password</b>	Enter the password for access to the Command Mode Enable level. There is no password by default.
<b>Quit connect line</b>	Enter a string to terminate a connect line session and resume the CLI. Type <b>&lt;control&gt;</b> before any key the user must press when holding down the <b>Ctrl</b> key. An example of a such a

Command Line Interface Configuration Settings	Description
	string is <control>L.

- Click **Submit**. Changes are applied immediately to the MatchPort b/g Pro.

## XML Configuration

The MatchPort b/g Pro allows for the configuration of units using an XML configuration file. Export a current configuration for use on other MatchPort b/g Pros or import a saved configuration file.

### XML: Export Configuration

On this 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 filesystem.

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

#### To export a system configuration record:

- Click **XML** on the menu bar and then **Export Configuration** at the top of the page. The XML Export Configuration page displays.



Figure 11-5. XML: Export Configuration

Export Configuration
Export Status
Import Configuration

## XML: Export Configuration

☐ Export XCR data to browser

☒ Export XCR data to the filesystem:

Filename

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

☒ 1
☒ 2
☒ 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:Line1_Modem_Ctl_In	<input checked="" type="checkbox"/> cp group:Line1_Modem_Ctl_O
<input checked="" type="checkbox"/> cp group:Line1_RS485_HDpx	<input checked="" type="checkbox"/> cp group:Line1_RS485_Select
<input checked="" type="checkbox"/> cp group:Line2_Modem_Ctl_In	<input checked="" type="checkbox"/> cp group:Line2_Modem_Ctl_O
<input checked="" type="checkbox"/> device	<input checked="" type="checkbox"/> email:1
<input checked="" type="checkbox"/> email:2	<input checked="" type="checkbox"/> email:3
<input checked="" type="checkbox"/> email:4	<input type="checkbox"/> ethernet:eth0
<input checked="" type="checkbox"/> firmware	<input checked="" type="checkbox"/> ftp server
<input checked="" type="checkbox"/> host:1	<input checked="" type="checkbox"/> host:2
<input checked="" type="checkbox"/> http authentication uri:/	<input checked="" type="checkbox"/> http server
<input checked="" type="checkbox"/> icmp	<input type="checkbox"/> interface:eth0
<input type="checkbox"/> interface:wlan0	<input checked="" type="checkbox"/> ip filter
<input checked="" type="checkbox"/> line	<input checked="" type="checkbox"/> lpd
<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"/> snmp	<input checked="" type="checkbox"/> ssh client
<input checked="" type="checkbox"/> ssh command mode	<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 command mode
<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"/> tunnel start	<input checked="" type="checkbox"/> tunnel stop
<input checked="" type="checkbox"/> wlan profile:adhoc	<input checked="" type="checkbox"/> wlan profile:default
<input checked="" type="checkbox"/> wlan profile:infrastructure	<input checked="" type="checkbox"/> wlan profile:profile1
<input checked="" type="checkbox"/> wlan profile:profile2	<input checked="" type="checkbox"/> wlan:wlan0
<input checked="" type="checkbox"/> xml import control	

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

The XML data can be exported to the browser window or to a file on the filesystem.

Notice that by default, all **Groups to Export** are checked except those pertaining to the network configuration; this is so that if you later "paste" the entire XML configuration, it will not break your network connectivity. You may check or uncheck any group to include or omit that group from export.

Selection of **Lines to Export** filters instances to be exported in the line, lpd, ppp, serial, tunnel ..., and terminal groups.

2. Enter or modify the following settings:

XML Export Configuration Page Settings	Description
Export XCR data to browser	Select this option to export the XCR data in the selected fields to a web browser.
Export XCR data to the filesystem	Select this option to export the XCR data to a filesystem. If you select this option, enter a file name for the XML configuration record.
Lines to Export	Select the instances you want to export in the line, lpd, serial, tunnel, and terminal groups.
Groups to Export	Check the configuration groups that are to be exported to the XML configuration record. If no groups are checked, all groups will be exported.

3. Click the **Export** button. The groups display if exporting the data to the browser. If exporting to the filesystem, the files are stored on the filesystem.

## 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 filesystem.

1. Click **XML** on menu bar and then **Export Status** at the top of the page. The XML Status Record: Export System Status page displays.

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

Export Configuration
Export Status
Import Configuration

### XML: Export Status

☐ Export XSR data to browser  
☒ Export XSR data to the filesystem:

Filename

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

☒ 1
 ☒ 2
 ☒ network

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

☒ arp  
☒ cp group  
☒ cps  
☒ email log:1  
☒ email log:3  
☒ email:1  
☒ email:3  
☒ filesystem  
☒ hardware  
☒ http log  
☒ interface:eth0  
☒ ip sockets  
☒ lpd  
☒ processes  
☒ rss  
☒ ssh  
☒ tcp  
☒ tftp  
☒ udp

☒ buffer pool  
☒ cp groups  
☒ device  
☒ email log:2  
☒ email log:4  
☒ email:2  
☒ email:4  
☒ ftp  
☒ http  
☒ icmp  
☒ ip  
☒ line  
☒ memory  
☒ query port  
☒ sessions  
☒ syslog  
☒ telnet  
☒ tunnel  
☒ xsr

This page is used for exporting the current system status in XML format.

The XML data can be exported to the browser window or to a file on the filesystem.

By default, all **Groups to Export** are checked, you may omit groups from export by unchecking them.

Selection of **Lines to Export** filters instances to be exported in the line, lpd, and tunnel groups.

2. Enter or modify the following settings:

XML Status Record: Export System Status Page Settings	Description
Export XSR data to browser	Select this option to export the XML status record to a web browser.
Export XSR data to the filesystem	Select this option to export the XML status record to a filesystem. If you select this option, enter a file name for the XML status record.
Lines to Export	Select the instances you want to export in the line, lpd, serial, tunnel, and terminal groups.
Groups to Export	Check the configuration groups that are to be exported into the XML status record. If no groups are checked, all groups will be exported.

3. Click the **Export** button. The groups display if exporting the data to the browser. If exporting to the filesystem, the files are stored on the filesystem.

## XML: Import System Configuration Page

Here you can import a system configuration from an XML file.

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

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

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

### To import a system configuration:

1. Click **XML** on the menu bar and then **Import Configuration** at the top of the page. The XML: Import Configuration page displays.

Figure 11-7. XML: Import Configuration

<p>Export Configuration   Export Status   <b>Import Configuration</b></p>	<p>This page is used for importing system configuration from an XML file.</p> <p><b>Import Configuration from External file</b> picks up all the settings from the external file.</p> <p><b>Import Configuration from Filesystem</b> picks up settings from the selected Groups, Lines and Instances. <b>Import Line(s) from single line Settings on the Filesystem</b> copies lines settings from an the input file containing only one Line instance to all of the selected Lines.</p> <p>When selecting a <b>Whole Groups to Import</b> item, all instances of that group will be imported. Notice that by default, all groups are checked except those pertaining to the network configuration; this is so that import will not break your network connectivity. You may check or uncheck any group to include or omit that group from import.</p> <p>Selection of <b>Lines to Import</b> filters instances to be imported in the line, lpd, ppp, serial, tunnel ..., and terminal groups. This affects both <b>Whole Groups to Import</b> and <b>Text List</b> selections.</p> <p>Use the <b>Text List</b> string to import specific instances of a group. The textual format of this string is:</p> <pre>&lt;g&gt;:&lt;i&gt;;&lt;g&gt;:&lt;i&gt;;...</pre> <p>Each group name &lt;g&gt; is followed by a colon and the instance value &lt;i&gt; and each &lt;g&gt;:&lt;i&gt; value is separated by a semi-colon. If a group has no instance then only the group name &lt;g&gt; should be specified.</p>
<h3>XML: Import Configuration</h3> <p><b>Import:</b></p> <ul style="list-style-type: none"> <li><input type="radio"/> Configuration from External file</li> <li><input type="radio"/> Configuration from Filesystem</li> <li><input type="radio"/> Line(s) from single line Settings on the Filesystem</li> </ul>	

### **Import Configuration from External File**

This selection displays 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 11-8. XML: Import Configuration from External File**

The screenshot shows a web interface for importing configuration. At the top, there are three tabs: 'Export Configuration', 'Export Status', and 'Import Configuration', with the latter being selected. Below the tabs, the main heading is 'XML: Import Configuration'. Under this heading, the text reads 'Import configuration from (entire) external XCR file:'. Below this text is a text input field and a 'Browse...' button. At the bottom left of the main content area is an 'Import' button. On the right side of the interface, there is a help text area that states: 'This page is used for importing system configuration from an XML file. Import Configuration from External file picks up all the settings from the external file. Import Configuration from Filesystem picks up settings from the selected Groups, Lines and Instances. Import Line(s) from single line Settings on the Filesystem copies lines settings from an the input file containing only one Line instance to all of the selected Lines.'

### **Import Configuration from the Filesystem**

This selection displays a page for entering the filesystem and your import requirements – groups, lines, and instances. Enter the filename of the XCR file that has certain groups you want to import.

Figure 11-9. XML: Import from Filesystem

Export Configuration
Export Status
Import Configuration

## XML: Import Configuration

**Import configuration from the filesystem:**

Filename

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

☒ 1
 ☒ 2
 ☒ network

**Whole Groups to Import:** [\[Clear All\]](#) [\[Select All but Networking\]](#)

<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"/> email	<input 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 filter	<input checked="" type="checkbox"/> line
<input checked="" type="checkbox"/> lpd	<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"/> snmp
<input checked="" type="checkbox"/> ssh client	<input checked="" type="checkbox"/> ssh command mode
<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 command mode	<input checked="" type="checkbox"/> terminal
<input checked="" type="checkbox"/> test	<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"/> tunnel start	<input checked="" type="checkbox"/> tunnel stop
<input checked="" type="checkbox"/> wlan	<input checked="" type="checkbox"/> wlan profile
<input checked="" type="checkbox"/> xml import control	

**Text List**

Import

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

**Import Configuration from External file** picks up all the settings from the external file.

**Import Configuration from Filesystem** picks up settings from the selected Groups, Lines and Instances. **Import Line(s) from single line Settings on the Filesystem** copies lines settings from an the input file containing only one Line instance to all of the selected Lines.

When selecting a **Whole Groups to Import** item, all instances of that group will be imported. Notice that by default, all groups are checked except those pertaining to the network configuration; this is so that import will not break your network connectivity. You may check or uncheck any group to include or omit that group from import.

Selection of **Lines to Import** filters instances to be imported in the line, lpd, ppp, serial, tunnel ..., and terminal groups. This affects both **Whole Groups to Import** and **Text List** selections.

Use the **Text List** 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 only the group name <g> should be specified.

## XML: Import Configuration from Filesystem

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

**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.

Figure 11-10. XML: Import Line(s) from Single Line Settings on the Filesystem

Export Configuration
Export Status
Import Configuration

## XML: Import Configuration

Import Line(s) from single line settings on the filesystem:

Filename

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

☒ 1
☒ 2
☒ network

Whole Groups to Import: [\[Clear All\]](#) [\[Select All but Networking\]](#)

<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"/> email	<input 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 filter	<input checked="" type="checkbox"/> line
<input checked="" type="checkbox"/> lpd	<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"/> snmp
<input checked="" type="checkbox"/> ssh client	<input checked="" type="checkbox"/> ssh command mode
<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 command mode	<input checked="" type="checkbox"/> terminal
<input checked="" type="checkbox"/> test	<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"/> tunnel start	<input checked="" type="checkbox"/> tunnel stop
<input checked="" type="checkbox"/> wlan	<input checked="" type="checkbox"/> wlan profile
<input checked="" type="checkbox"/> xml import control	

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

Import Configuration from External file picks up all the settings from the external file. Import Configuration from Filesystem picks up settings from the selected Groups, Lines and Instances. Import Line(s) from single line Settings on the Filesystem copies lines settings from an the input file containing only one Line instance to all of the selected Lines.

When selecting a Whole Groups to Import item, all instances of that group will be imported. Notice that by default, all groups are checked except those pertaining to the network configuration; this is so that import will not break your network connectivity. You may check or uncheck any group to include or omit that group from import.

Selection of Lines to Import filters instances to be imported in the line, lpd, ppp, serial, tunnel ..., and terminal groups. This affects both Whole Groups to Import and Text List selections.

Use the Text List 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 only the group name <g> should be specified.



## XML: Import Lines from Single Line(s) Settings

Import Line( s) Settings	Description
Filename	Provide the name of the file on the MatchPort b/g Pro (local to its file system) that contains XCR data.
Lines to Import	Select the line(s) whose settings you want to import. Click the <b>Select All</b> link to select all the serial lines and the network lines. Click the <b>Clear All</b> link clear all of the checkboxes. By default, all serial line instances are selected.
Whole Groups to Import	<p>Select the configuration groups to import from the XML configuration record.</p> <p><b>Note:</b> <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></p> <p>You may check or uncheck any group to include or omit that group from import. To import all of the groups, click the <b>Select All</b> link to import all groups. To clear all the checkboxes, click the <b>Clear All</b> link.</p>

## 12: Point-to-Point Protocol (PPP)

**Note:** For instructions on configuring PPP for the MatchPort b/g Pro, see [PPP](#) on page 81.

Point-to-Point Protocol (PPP) establishes a direct connection between two nodes. It defines a method for data link connectivity between devices using physical layers (such as serial lines). Some of the PPP features include error detection, compression, and authentication. For each of these capabilities, PPP has a separate protocol.

The MatchPort b/g Pro supports two types of PPP authorization: Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP). Both of these authentication methods require the configuration of a username and password. It also supports no authentication scheme when no authentication is required during link negotiation.

PAP is an authentication protocol in PPP. It 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.

**Note:** PAP is not a strong authentication process. There is no protection against trial-and-error attacks. As well, the peer is responsible for the frequency of the 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.

Use the MatchPort b/g Pro's 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 b/g Pro 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 between the serial-side network interface and the Ethernet/WLAN network interface. Therefore, to pass packets through the MatchPort b/g Pro, a static route must be configured on both the PPP Peer device and the remote device it wishes to communicate with. The static route in the PPP Peer device must use the PPP Local IP Address as its gateway, and the static route in the remote device must use the Ethernet/WLAN IP Address of the MatchPort b/g Pro as its gateway.

## 13: Tunneling

Serial tunneling allows devices to communicate over a network, without detecting other devices connecting between them. Tunneling parameters are configured using the Web Manager's [Tunnel 1 and Tunnel 2 Settings](#) (on page 57) or Command Mode's Tunnel Menu (see 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 the other 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's 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).

### Connect Mode

For Connect Mode to function, it must be enabled, have a remote station (node) configured, and a remote port configured (TCP or UDP). When enabled, Connect Mode is always on.

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

Connect Mode supports the following protocols:

- ◆ TCP
- ◆ AES encryption over UDP
- ◆ AES encryption over TCP
- ◆ SSH (the MatchPort b/g Pro is the SSH client)

- ◆ UDP (available only in Connect Mode because it is a connectionless protocol).

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.

For Connect Mode using UDP, if the remote address or port is not configured, then 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. As a result, we advise configuring the remote address and port. When the remote port and station are configured, the MatchPort b/g Pro ignores data from other sources.

**Note:** *The Local Port in Connect Mode is not the same port configured in Accept Mode.*

To ignore data sent to the MatchPort b/g Pro, enable the blocking of serial data or network data (or both).

The TCP keepalive time is the time in which probes are periodically sent to the other end of the connection. This ensures the other side is still connected.

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's SSH client username is configured on the remote SSH server before using it with the MatchPort b/g Pro.

Connect Mode has five states:

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

For the “any character” or “specific character” connection states, 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 any character or the start character again (depending on the configured setting).

Configure the Modem Control Active 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.

## Accept Mode

In Accept Mode, the MatchPort b/g Pro waits for a connection. The configurable local port is the port the remote device connects to for this connection. There is no remote port or address. The default local port is 10001 for serial port 1 and 10002 for serial port 2.

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.
- ◆ TCP
- ◆ AES encryption over TCP
- ◆ Telnet/IAC mode (The MatchPort b/g Pro currently supports IAC codes. It drops the IAC codes when Telneting and does not forward them to the serial port).

Accept Mode has the following states:

- ◆ Disabled (close the connection)
- ◆ Enabled (always listening for a connection)
- ◆ Active if it receives any character from the serial port
- ◆ Active if it receives a specific (configurable) character from the serial port (same start character as Connect Mode's start character)
- ◆ Modem control signal
- ◆ Modem emulation

## Disconnect Mode

Disconnect Mode ends Accept Mode and Connect Mode connections. When disconnecting, the MatchPort b/g Pro shuts down connections gracefully.

The following settings end a 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.
- ◆ The MatchPort b/g Pro observes the modem control inactive setting.

To clear data out of the serial buffers upon a disconnect, configure buffer flushing.

## Packing Mode

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

The following settings are configurable for Packing Mode:

- ◆ Disable Packing Mode
- ◆ Packing Mode timeout: The data is packed for a specified period before being sent out.
- ◆ Packing Mode threshold: When the buffer fills to a specified amount of data (and the timeout has not elapsed), the MatchPort b/g Pro packs the data and sends it out.
- ◆ The send character: Similar to a start or stop character, the MatchPort b/g Pro packs the data until it sees the send character. The MatchPort

b/g Pro then sends the packed data and the send character in the packet.

- ◆ A trailing character: If a trailing character is defined, this character is appended to data put on the network immediately following the send character.

## Modem Emulation

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

**Command Mode:** sends back verbal response codes.

**Data Mode:** information transferred in is also transferred out.

It is possible to change the default on bootup for verbose response codes, echo commands, and quiet mode. The current settings can be overridden; however on reboot, it will go back to the programmed settings.

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

### Command Mode

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

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

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.

**Note:** Configure either the IP address using the address on its own (<xxx.xxx.xxx.xxx>), or the IP address and port number by entering <xxx.xxx.xxx.xxx>:<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 Command Mode. Once Command Mode is exited, 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 plus** command.

## Serial Line Settings

Serial line settings are configurable for both serial line 1 and serial line 2.

Configure the buffer size to change the maximum amount of data the serial port stores. For any active connection, the MatchPort b/g Pro sends the data in the buffer. The read timeout is used for periodically sending data. If the buffer is not full (reached the buffer size) but the read timeout time has elapsed, the data in the buffer is sent out.

## Statistics

The MatchPort b/g Pro logs statistics for tunneling. The **Dropped** statistic displays connections ended by the remote location. The **Disconnected** statistic displays connections ended by the MatchPort b/g Pro.



## 14: Security in Detail

The MatchPort b/g Pro supports Secure Shell (SSH) and Secure Sockets Layer (SSL).

### Secure Shell: SSH

SSH is a network protocol for securely accessing a remote device. This protocol provides a secure, encrypted communication channel between two hosts over a network.

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.

### SSH Server Configuration

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's SSH server.

#### To configure SSH server settings:

1. Click **SSH → Server Host Keys** at the top of the page. The SSH Server: Host Keys page displays.
2. To configure the host keys:
  - a) If the keys exist, locate the **Private Key** and **Public Key** using the **Browse** button. Select the **Key Type** (RSA is more secure) and click **Submit** to upload the keys.

**Note:** SSH keys may be created on another computer and uploaded to the MatchPort b/g Pro. To do so, use the following command using Open SSH to create a 1024-bit DSA key pair:

```
ssh-keygen -b 1024 -t dsa
```

- b) SSH Keys from other programs may be converted to the required MatchPort b/g Pro format. Use Open SSH to perform the conversion. To convert from RFC-4716 format:

```
ssh-keygen -i
```

For more options, look at the help from Open SSH:

```
ssh-keygen ?
```

- c) If the keys do not exist, select the **Key Type** and the key's **Bit Size** from the **Create New Keys** section. Click **Submit** to create new private and public host keys.

**Note:** *Generating new keys with a large bit size results in very long key generation time.*

3. Click **SSH → Server Auth Users** at the top of the page. The SSH Server: Authorized Users page displays.
4. Enter the **Username** and **Password** for authorized users.
5. If available: locate the **Public RSA Key** or the **Public DSA Key** by clicking **Browse**. Configuring a public key results in public key authentication; this bypasses password queries.

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

## SSH Client Configuration

To configure the MatchPort b/g Pro as an SSH client, there is one requirement:

- ◆ An SSH client user is configured and exists on the remote SSH server.

### To configure SSH client settings:

1. Click **SSH → Client Users** at the top of the page. The SSH Client: Users page displays.
2. (Required) Enter the **Username** and **Password** to authenticate with the SSH server.
3. (Optional) Complete the SSH client user information as necessary. The **Private Key** and **Public Key** automate the authentication process; when configured and the user public key is known on the remote SSH server, the SSH server does not require a password. (Alternatively, generate new keys using the **Create New Keys** section.) The **Remote Command** is provided to the SSH server. 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.*

## Secure Sockets Layer (SSL)

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 SSLv3 and its successors, TLS1.0 and TLS1.1.

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

### CipherSuites

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.

MatchPort b/g Pro currently supports the following list of 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.

### Certificates

#### Principles

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.

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's 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 become one's own CA. Tools exist to generate self-signed CA certificates or to sign other certificates.

A certificate before it is signed is known as a certificate request, which only contains the identifying information. Signing it makes it a certificate. One's certificate is also used to sign any message transmitted to the peer to identify the originator and prevent tampering while transported.

In short:

- ◆ When using HTTPS, SSL Tunneling in Accept mode, and/or EAP-TLS, the MatchPort b/g Pro needs a personal certificate with 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(s) that can authenticate those it wishes to communicate with.

## 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.

## Obtaining a Certificate and Private Key

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. (See [Error! Reference source not found. on page Error! Bookmark not defined.](#)) 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.

Several utilities exist to convert between the formats.

## Utilities

### OpenSSL

Openssl is a widely used 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 from and to all kinds of formats.

Executables are available 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](http://www.openssl.org) or [www.madboa.com/geek/openssl](http://www.madboa.com/geek/openssl) for more information.

**Note:** *Signing other certificate requests is also possible with OpenSSL but is too complicated to explain here.*

### Steel Belted Radius

Steel Belted Radius is a 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:

```
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. Open the file in any plain text editor. 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. We will add support for this and other formats in future releases.*

### FreeRadius

Free Radius is a Linux open-source Radius server. It is versatile, but a little complicated to configure, requiring the user to be knowledgeable.

## 15: Branding the MatchPort b/g Pro

The MatchPort b/g Pro's Web Manager and Command Mode (CLI) are customizable.

### Web Manager Customization

Customize the Web Manager's appearance by modifying the following files:

**Note:** To view these files, open the **http → config** folder using the Filesystem Browser. Alternatively, upload and download the files using FTP/TFTP.

Filename	Description
<b>index.css</b>	The Web Manager's style sheet.
<b>footer.html</b>	Formats the web page's footer.
<b>header.html</b>	Formats the web page's header.
<b>ltrx_logo.gif</b>	The Lantronix logo within the header. To replace the logo, ensure the replacement logo's height is 70 pixels.
<b>bg.gif</b>	The background image file. The background is tiled.

### Command Mode

Customize the MatchPort b/g Pro's Command Mode by changing its short name and long name. The short name is used for show commands:

```
(enable)# show MatchPort
```

The long name appears in the Product Type field:

```
(enable)# show MatchPort
Product Information:
    Product Type: Lantronix MatchPort b/g Pro
```

**To change the MatchPort b/g Pro's short and long names:**

1. Click **System** at the top of the page. The System page opens.
2. In the **Short Name** field, enter the new short name for the device (up to 32 characters).
3. In the **Long Name** field, enter the new long name for the device (up to 64 characters).
4. Click **Submit**.
5. To apply changes, click **Reboot**.

## 16: Updating Firmware

### Obtaining Firmware

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

### Loading New Firmware

Reload the firmware using the MatchPort b/g Pro's Web Manager's Filesystem page.

**To upload new firmware:**

1. Click **System** in the menu bar. The Filesystem page opens.
2. In the **Upload New Firmware** section, click **Browse**. A pop-up page displays; locate the firmware file.
3. Click **Upload** to install the firmware on the MatchPort b/g Pro. The device automatically reboots upon the installation of new firmware.

## ***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 1 39 30 41 72

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

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

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

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



## B: 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 hexadecimal or to look up hexadecimal values in the tables of configuration options. The tables include:

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

### Converting Binary to Hexadecimal

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

#### Conversion Table

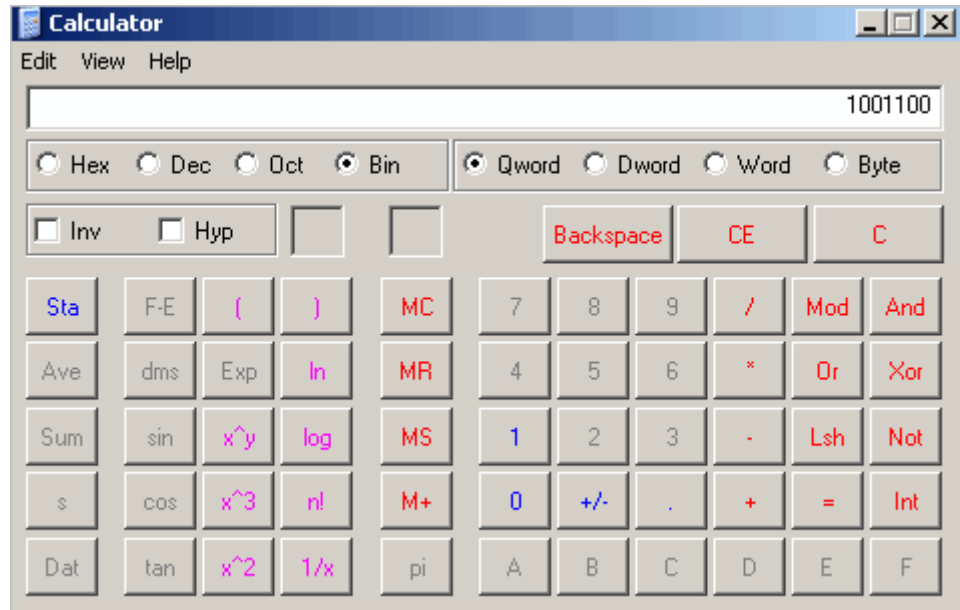
Hexadecimal digits have values ranging from 0 to F, which are represented as 0-9, A (for 10), B (for 11), etc. To convert a binary value (for example, 0100 1100) to a hexadecimal representation, treat the upper and lower four bits separately to produce a two-digit hexadecimal number (in this case, 4C).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

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

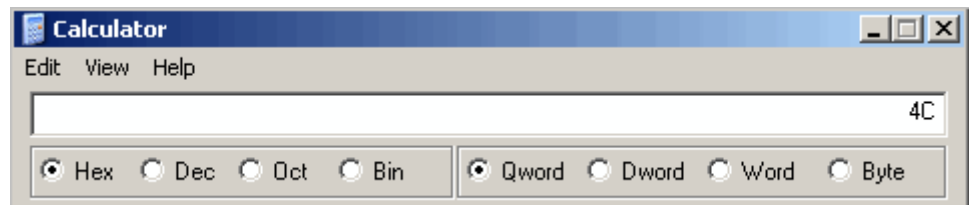
## Scientific Calculator

Another simple way to convert binary to hexadecimal is to use a scientific calculator, such as the one available on 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 displays.
3. Click **Bin** (Binary), and type the number you want to convert.



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



## ***C: Warranty***

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