MatchPort AR
User Guide

Part Number 900-480
Revision A June 2007

Copyright & Trademark

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

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

Disclaimer & 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
6/2007	A	Initial Document

Contents

Figures

1: Using This Guide

Purpose and Audience

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

Summary of Chapters

The remaining chapters in this guide include:

Chapter	Description
2: Introduction	Main features of the product and the protocols it supports. Includes technical specifications.
3: Using DeviceInstaller	Instructions for viewing the current configuration using DeviceInstaller.
4: Configuration Using Web Manager	Instructions for accessing Web Manager and using it to configure settings for the MatchPort AR.
5: Point-to-Point Protocol (PPP)	Description of PPP on the MatchPort AR.
6: Tunneling	Information about tunneling features available on the serial lines.
7: SSH and SSL Security	Description and configuration of SSH and SSL security settings.
8: Email	Information about the SMTP server and setting email parameters on the MatchPort AR.
9: Configuration Pin Manager	Information about the Configuration Pin Manager (CPM) and how to set the configurable pins to work with a device.
10: XML	Information about configuring the MatchPort AR using XML.
11: Branding the MatchPort AR	Instructions for customizing the MatchPort AR.
12: Updating Firmware	Instructions for obtaining the latest firmware and updating the MatchPort AR.
A: Technical Support	Instructions for contacting Lantronix Technical Support.
B: Binary to Hexadecimal	Instructions for converting binary values to hexadecimals.
C: Warranty	Lantronix's warranty statement.

Additional Documentation

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

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

2: Introduction

This chapter summarizes the MatchPort AR device server's features and basic information you need before getting started.

Features

The MatchPort AR has the following features:

- The Evolution OS operating system
- 2 full serial ports with all hardware handshaking signals
- 7 configurable pins
- 4 MB Flash and 8 MB RAM memory

Applications

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

- ATM machines
- CNC controllers
- Data collection devices
- Universal Power Supply (UPS) management units
- Telecommunications equipment
- Data display devices
- Security alarms and access control devices
- Handheld instruments
- Modems
- Time/attendance clocks and terminals

Protocol Support

The MatchPort AR 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, SSH, SSL, SNMP, and SMTP for network communications and management.

- TCP, UDP, TCP/AES, UDP/AES, Telnet, SSH and SSL for tunneling to the serial port.
- TFTP, FTP, and HTTP for firmware upgrades and uploading files.

Evolution OS™

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

Web-Based Configuration and Troubleshooting

Built upon popular Internet-based standards, the MatchPort AR 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 AR 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 AR supports full SNMP management, making it ideal for applications where device management and monitoring are critical. These features allow networks with SNMP capabilities to correctly diagnose and monitor MatchPort AR.

XML-Based Architecture and Device Control

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

Rich Site Summary (RSS)

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

Enterprise-Grade Security

Without the need to disable any features or functionality, the Evolution OS™ provides the MatchPort AR 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 being transmitted across public networks, users can maintain their existing investment in serial technology, while taking advantage of the highest data-protection levels possible.

SSH and SSL can:

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

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

You can use the MatchPort AR with 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.

Troubleshooting Capabilities

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

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

Configuration Methods

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

DeviceInstaller: Configure the IP address and related settings and view current settings on the MatchPort AR using a Graphical User Interface (GUI) on a PC attached to a network. (See *3: Using DeviceInstaller*.)

Web Manager: Through a web browser, configure the MatchPort AR'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 AR Command Reference Guide for instructions and available commands.*)*

XML: The MatchPort AR supports XML-based configuration and setup records that make device configuration transparent to users and administrators. The XML is easily editable with a standard text or XML editor. (See the MatchPort AR 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 AR:

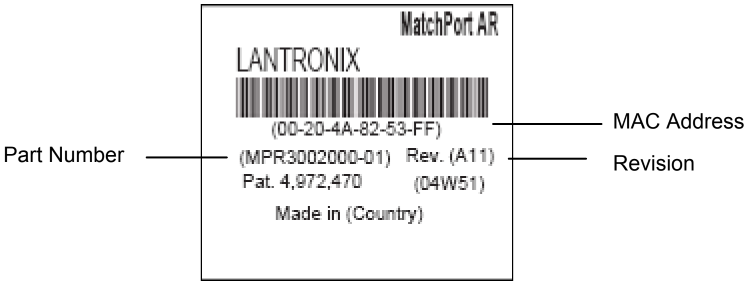
- TCP Port 22: SSH Server (Command Mode configuration)
- TCP Port 23: Telnet Server (Command Mode configuration)
- TCP Port 80: HTTP (Web Manager configuration)
- TCP Port 443: HTTPS (Web Manager configuration)
- UDP Port 161: SNMP
- TCP Port 21: FTP
- UDP Port 69: TFTP
- UDP Port 30718: LDP (Lantronix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

Product Information Label

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 AR 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.

Accessing MatchPort AR using DeviceInstaller

Note: Make note of the MAC address. It is needed to locate the MatchPort AR 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 AR devices available displays.
3. Expand the list of MatchPorts by clicking the **+** symbol next to the MatchPort AR icon. Select the MatchPort AR unit by clicking its IP address to view its configuration.

Viewing the MatchPort AR's Current Configuration

1. In the right page, click the **Device Details** tab. The current MatchPort AR configuration displays:

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

Current Settings	Description
Name	Name identifying the MatchPort AR.
Group	Configurable field. Enter a **group** to categorize the MatchPort AR. Double-click the field, type in the value, and press **Enter** to complete. This group name is not visible on other PCs or laptops using DeviceInstaller.
Comments	Configurable field. Enter **comments** for the MatchPort AR. Double-click the field, type in the value, and press **Enter** to complete. This description or comment is local to this PC and is not visible on other PCs or laptops using DeviceInstaller.
Device Family	Displays the MatchPort AR's device family type as **MatchPort**.
Type	Displays the device type as **MatchPort AR**.
ID	Displays the MatchPort AR's ID embedded within the unit.
Hardware Address	Displays the MatchPort AR's hardware (MAC) address.

Current Settings	Description
Firmware Version	Displays the firmware currently installed on the MatchPort AR.
Extended Firmware Version	Provides additional information on the firmware version.
Online Status	Displays the MatchPort AR's status as online, offline, unreachable (the MatchPort AR is on a different subnet), or busy (the MatchPort AR is currently performing a task).
Telnet Enabled	Indicates whether Telnet is enabled on this MatchPort AR.
Telnet Port	Displays the MatchPort AR's port for Telnet sessions.
Web Enabled	Indicates whether Web Manager access is enabled on this MatchPort AR.
Web Port	Non-configurable field. Displays the MatchPort AR's port for Web Manager configuration.
Maximum Baud Rate Supported	Displays the MatchPort AR's maximum baud rate.
Firmware Upgradeable	Displays **True**, indicating the MatchPort AR's firmware is upgradeable as newer version become available.
IP Address	Displays the MatchPort AR's current IP address. To change the IP address, click the **Assign IP** button on the DeviceInstaller menu bar.
IP Address was Obtained	Displays **Dynamically** if the MatchPort AR automatically received an IP address (e.g., from DHCP). Displays **Statically** if the IP address was entered manually. If the IP address was assigned dynamically, 2-4 of the following fields display: **Obtain via DHCP** with values of **True** or **False**. **Obtain via BOOTP** with values of **True** or **False**. **Obtain via RARP** with values of **True** or **False**. **Obtain via AutoIP** with values of **True** or **False**.
Subnet Mask	Displays the subnet mask specifying the network segment on which the MatchPort AR resides.
Gateway	Displays the IP address of the router of this network. There is no default.
Number of Ports	Displays the number of ports on this MarchPort AR.
Supports Configurable Pins	Displays **True**, indicating configurable pins are available on the MatchPort AR.
Supports Email Triggers	Displays **True**, indicating email triggers are available on the MatchPort AR.

4: Configuration Using Web Manager

This chapter describes how to configure the MatchPort AR 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 AR 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 AR in the address bar.

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

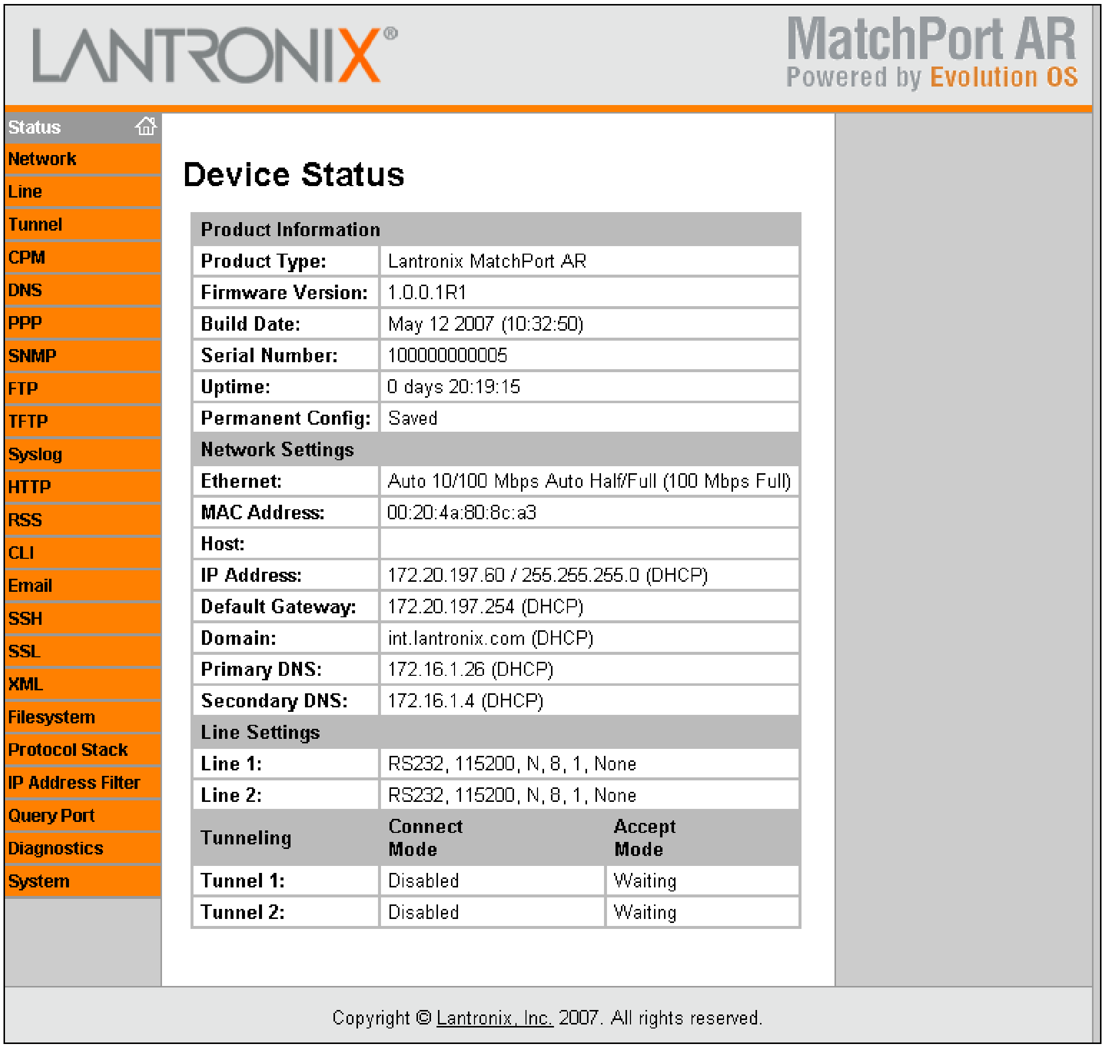
3. Enter your user name and password.

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

4. The Web Manager home page displays.

Note: The MatchPort AR Status page (the home page) displays the common MatchPort AR configuration and product information.

Figure 4-1. Web Manager Home Page



Device Status

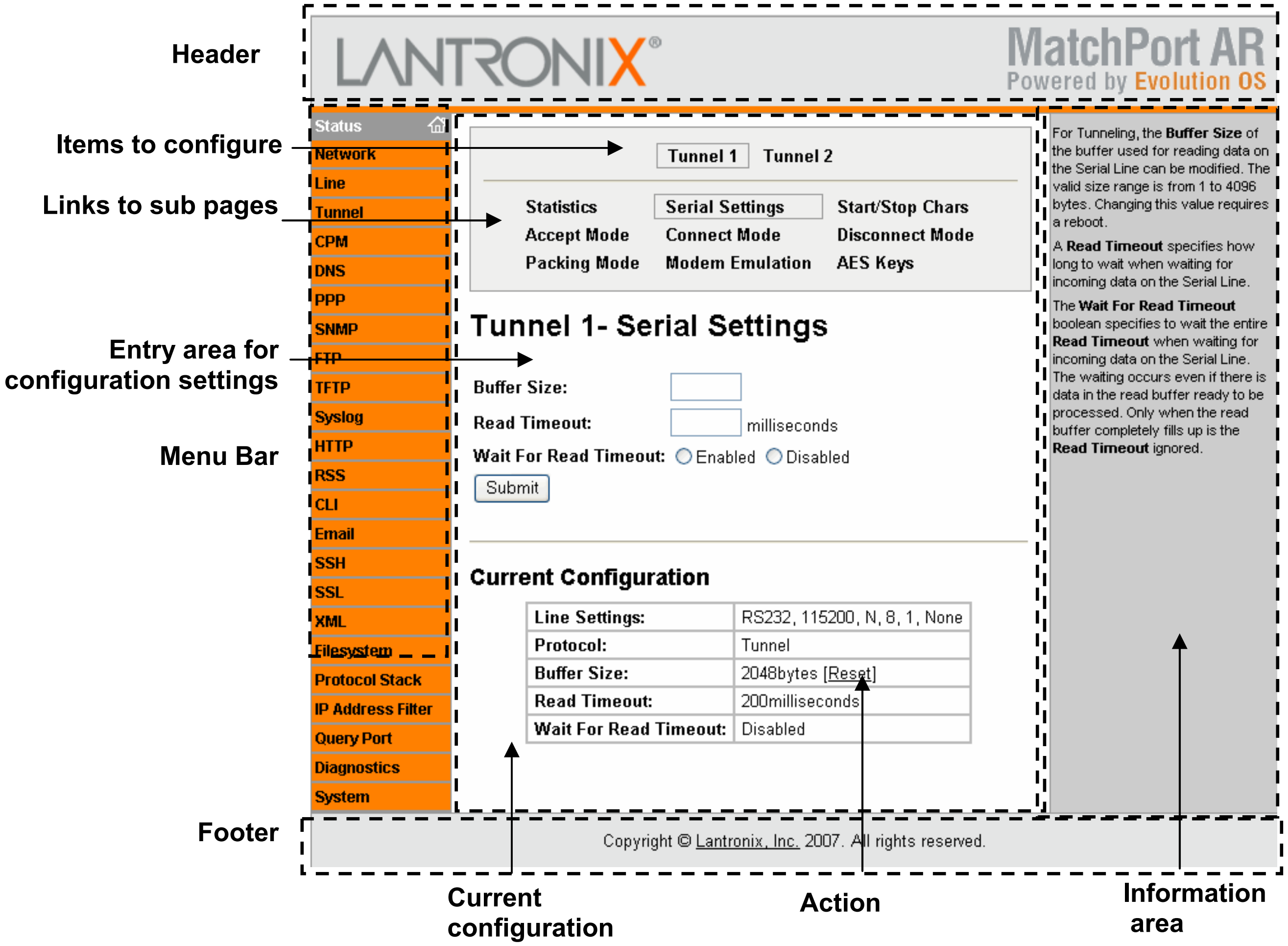
Product Information		
Product Type:	Lantronix MatchPort AR	
Firmware Version:	1.0.0.1R1	
Build Date:	May 12 2007 (10:32:50)	
Serial Number:	100000000005	
Uptime:	0 days 20:19:15	
Permanent Config:	Saved	
Network Settings		
Ethernet:	Auto 10/100 Mbps Auto Half/Full (100 Mbps Full)	
MAC Address:	00:20:4a:80:8c:a3	
Host:		
IP Address:	172.20.197.60 / 255.255.255.0 (DHCP)	
Default Gateway:	172.20.197.254 (DHCP)	
Domain:	int.lantronix.com (DHCP)	
Primary DNS:	172.16.1.26 (DHCP)	
Secondary DNS:	172.16.1.4 (DHCP)	
Line Settings		
Line 1:	RS232, 115200, N, 8, 1, None	
Line 2:	RS232, 115200, N, 8, 1, None	
Tunneling	**Connect Mode**	**Accept Mode**
Tunnel 1:	Disabled	Waiting
Tunnel 2:	Disabled	Waiting

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

Understanding the Web Manager Pages

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

Figure 4-2. Components of the Web Manager Page



Tunnel 1- Serial Settings

Buffer Size:

Read Timeout: milliseconds

Wait For Read Timeout: ○ Enabled ○ Disabled

Current Configuration

Line Settings:	RS232, 115200, N, 8, 1, None
Protocol:	Tunnel
Buffer Size:	2048bytes [Reset]
Read Timeout:	200milliseconds
Wait For Read Timeout:	Disabled

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

A **Read Timeout** specifies how long to wait when waiting for incoming data on the Serial Line.

The **Wait For Read Timeout** boolean specifies to wait the entire **Read Timeout** when waiting for incoming data on the Serial Line. The waiting occurs even if there is data in the read buffer ready to be processed. Only when the read buffer completely fills up is the **Read Timeout** ignored.

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

- 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 AR 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.

Network Settings

Click **Network** on the menu bar to display the Network page. Here you can change the following MatchPort AR network configuration settings:

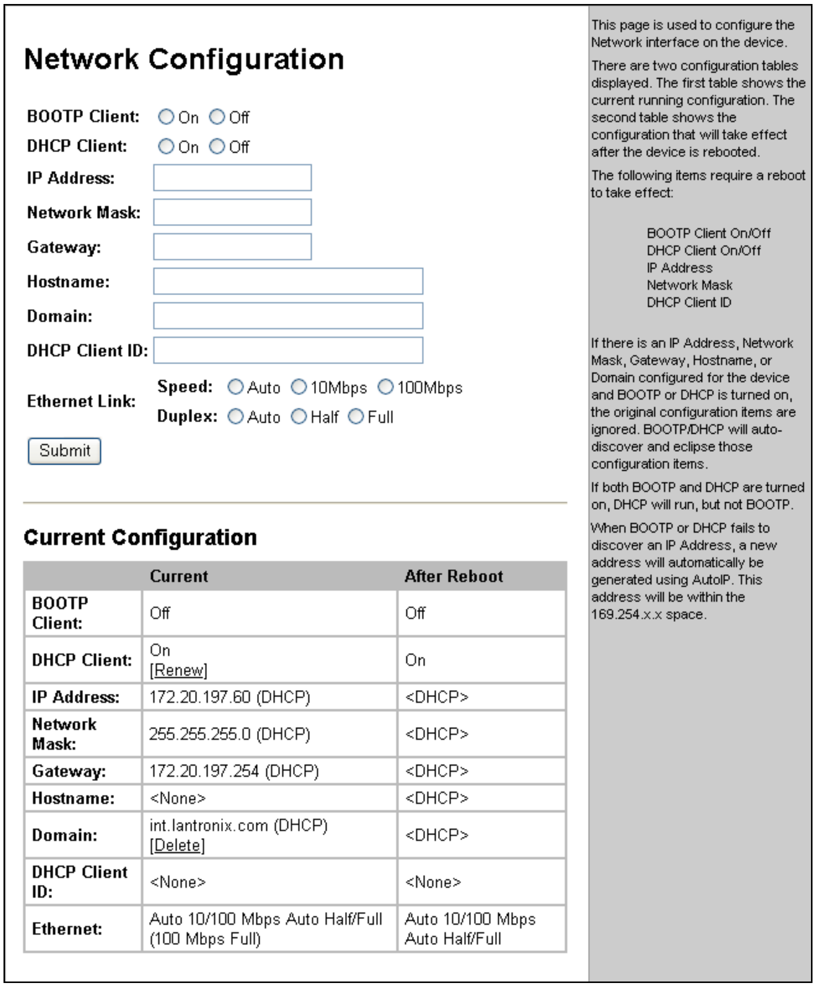
- BOOTP and DHCP client
- IP address, network mask, and gateway
- Hostname and domain
- DHCP client ID
- Ethernet transmission speed

Network Configuration

To configure the network's general configuration:

1. Click **Network** on the menu bar. The Network Configuration page displays.

Figure 4-3. Network Configuration



Network Configuration

BOOTP Client: ○ On ○ Off

DHCP Client: ○ On ○ Off

IP Address:

Network Mask:

Gateway:

Hostname:

Domain:

DHCP Client ID:

Ethernet Link: Speed: ○ Auto ○ 10Mbps ○ 100Mbps
Duplex: ○ Auto ○ Half ○ Full

Current Configuration

	Current	After Reboot
BOOTP Client:	Off	Off
DHCP Client:	On [Renew]	On
IP Address:	172.20.197.60 (DHCP)	<DHCP>
Network Mask:	255.255.255.0 (DHCP)	<DHCP>
Gateway:	172.20.197.254 (DHCP)	<DHCP>
Hostname:	<None>	<DHCP>
Domain:	int.lantronix.com (DHCP) [Delete]	<DHCP>
DHCP Client ID:	<None>	<None>
Ethernet:	Auto 10/100 Mbps Auto Half/Full (100 Mbps Full)	Auto 10/100 Mbps Auto Half/Full

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

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

The following items require a reboot to take effect:

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

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

If both BOOTP and DHCP are turned on, DHCP 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.

2. Enter or modify the following settings:

Network - Configuration Page Settings	**Description**
BOOTP Client	Select **On** or **Off**. Overrides the configured IP address, network mask, gateway, hostname, and domain. *Note: When DHCP is set to **On**, the system automatically uses DHCP, regardless of whether BOOTP Client is set to **On.***
DHCP Client	Select **On** or **Off**. Overrides the configured IP address, network mask, gateway, hostname, and domain. *Note: A link in the Current Configuration section of the page enables you to renew DHCP Client.*
IP Address	Enter the MatchPort AR's static IP address. The IP address consists of four octets separated by a period and is used if BOOTP and DHCP are both set to **Off**. Changing this value requires you to reboot the MatchPort AR. *Note: When DHCP is enabled, the MatchPort AR tries to obtain an IP address from DHCP. If it cannot, the MatchPort AR uses an Auto IP address in the range of 169.254.xxx.xxx.*

Network - Configuration Page Settings	Description
Network Mask	Enter the MatchPort AR's network mask. The subnet mask consists of four octets separated by a period. Changing this value requires you to reboot the MatchPort AR. ***Note:*** *When DHCP is enabled, the MatchPort AR tries to obtain a network mask from DHCP. If it cannot, it uses a network mask of 255.255.0.0.*
Gateway	Enter the MatchPort AR's gateway address.
Hostname	Enter the MatchPort AR's hostname.
Domain	Enter the MatchPort AR's domain name. ***Note:*** *A link in the Current Configuration section of the page enables you to delete the domain name.*
DHCP Client ID	Enter the ID if a DHCP ID is used by the DHCP server. 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 AR's MAC address.
Ethernet Link Speed	Select the Ethernet link speed. (Default is **Auto**.)
Ethernet Link Duplex	Select duplex mode. (Default is **Auto**.)

3. In the **Current Configuration** table, delete currently stored settings as necessary.

4. Click **Submit**. Some changes are applied immediately to the MatchPort AR. Changes to the following settings require a reboot for the changes to take effect: DHCP, BOOTP, IP address, network mask, gateway, MAC address, and 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.*

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.

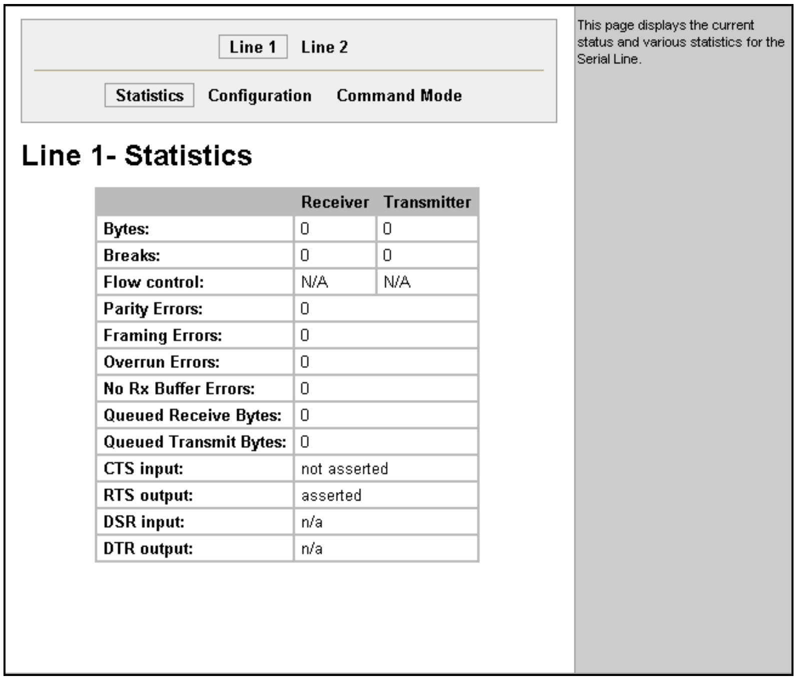
Note: *The following section describes the steps to view and configure Line 1 settings; these steps also apply to Line 2 menu options*.

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 4-4. Line 1 Statistics



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

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	

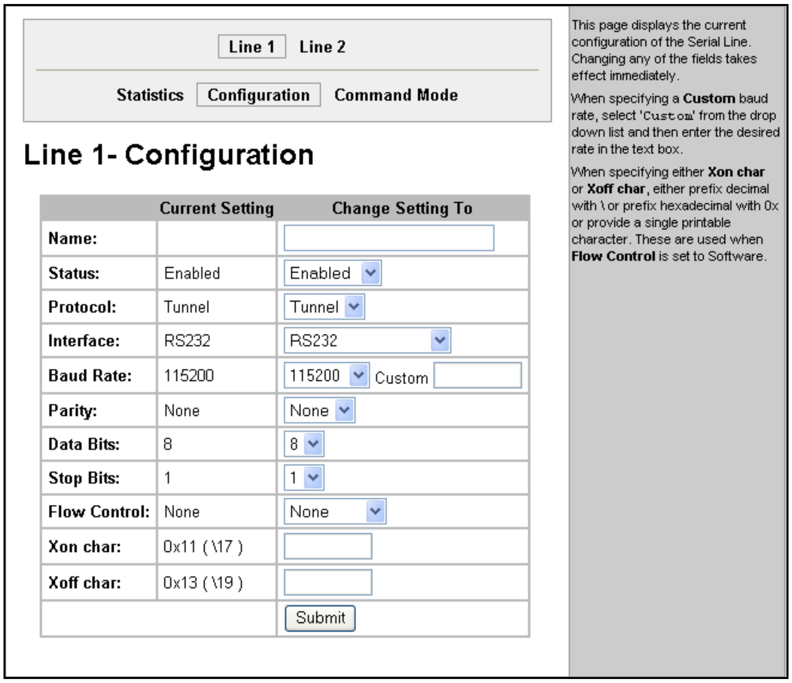
Line 1 Configuration

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 4-5. Line 1 Configuration



Line 1- Configuration

	Current Setting	Change Setting To
Name:		
Status:	Enabled	Enabled
Protocol:	Tunnel	Tunnel
Interface:	RS232	RS232
Baud Rate:	115200	115200 Custom
Parity:	None	None
Data Bits:	8	8
Stop Bits:	1	1
Flow Control:	None	None
Xon char:	0x11 (\17)	
Xoff char:	0x13 (\19)	
		Submit

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

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

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

2. Enter or modify the following settings:

Line - Configuration Page Settings	Description
Name	Enter a name for the line. The default **Name** is blank.
Status	Indicates whether the current line is enabled. To change the status, select Enabled or **Disabled** from the drop-down menu.
Protocol	Select the protocol for the line from the drop-down menu. The default is **None**.
Interface	Select the line's interface from the drop-down menu. The default is **RS232**.
Baud Rate	Select the MatchPort AR's baud rate from the drop-down menu. The default is **9600**.
Parity	Select the MatchPort AR's parity from the drop-down menu. The default is **None.**
Data Bits	Select the number of data bits from the drop-down menu. The default is **8**.
Stop Bits	Select the number of stop bits from the drop-down menu. The default is **1.**
Flow Control	Select the MatchPort AR's flow control from the drop-down menu. The default is **None.**
Xon Char	Specify the character to use to initiate a flow of data. When **Flow Control** is set to **Software**, specify **Xon char**. Prefix a decimal character with \ or a hexadecimal character with **0x**, or provide a single printable character. The default Xon char is **0x11**.
Xoff Char	When **Flow Control** is set to **Software**, specify **Xoff char**.

Line - Configuration Page Settings	Description
	Prefix a decimal character with \ or a hexadecimal character with **0x**, or provide a single printable character. The default Xoff char is **0x13**.

3. Click **Submit**. Changes are applied immediately to the MatchPort AR.

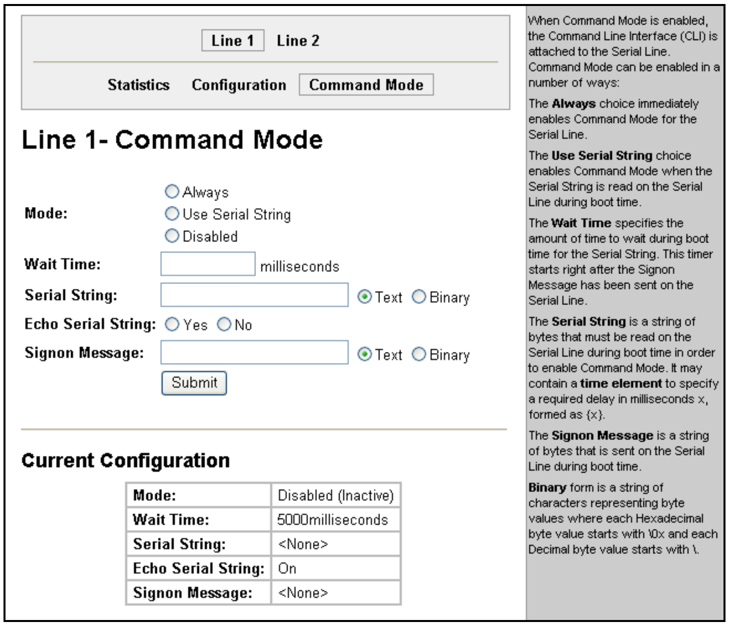
Line 1 Command Mode

Setting Command Mode enables the CLI on the serial line.

To configure Line 1's Command Mode:

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

Figure 4-6. Line 1 Command Mode



Line 1- Command Mode

Mode: ○ Always ○ Use Serial String ○ Disabled

Wait Time: ______ milliseconds

Serial String: ______ ● Text ○ Binary

Echo Serial String: ○ Yes ○ No

Signon Message: ______ ● Text ○ Binary

Submit

Current Configuration

Mode:	Disabled (Inactive)
Wait Time:	5000milliseconds
Serial String:	<None>
Echo Serial String:	On
Signon Message:	<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 **Wait Time** specifies the amount of time to wait during boot time for the Serial String. This timer starts right after the Signon Message has been sent on the Serial Line.

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

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

Binary form is a string of characters representing byte values where each Hexadecimal byte value starts with \0x and each Decimal byte value starts with \.

2. Enter or modify the following settings:

Line - Command Mode Page Settings	Description
Mode	Select the method of enabling Command Mode or choose to disable Command Mode. **Always** = immediately enables Command Mode for the serial line. **Use Serial String** = enables Command Mode when the serial string is read on the serial line during boot time. **Disabled** = turns off Command Mode.
Wait Time	Enter the wait time for the serial string during boot-up in milliseconds.

Line - Command Mode Page Settings	Description
Serial String	Enter the serial string characters. Select a string type of **Text** or **Binary** notation. 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 ****.
Echo Serial String	Select **Yes** to enable echoing of the serial string at boot-up.
Signon Message	Enter the boot-up signon message. Select a string type of **Text** or **Binary** notation.

3. In the **Current Configuration** table, clear currently stored settings as necessary.

4. Click **Submit**. Changes are applied immediately to the MatchPort AR.

Tunnel 1 and Tunnel 2 Settings

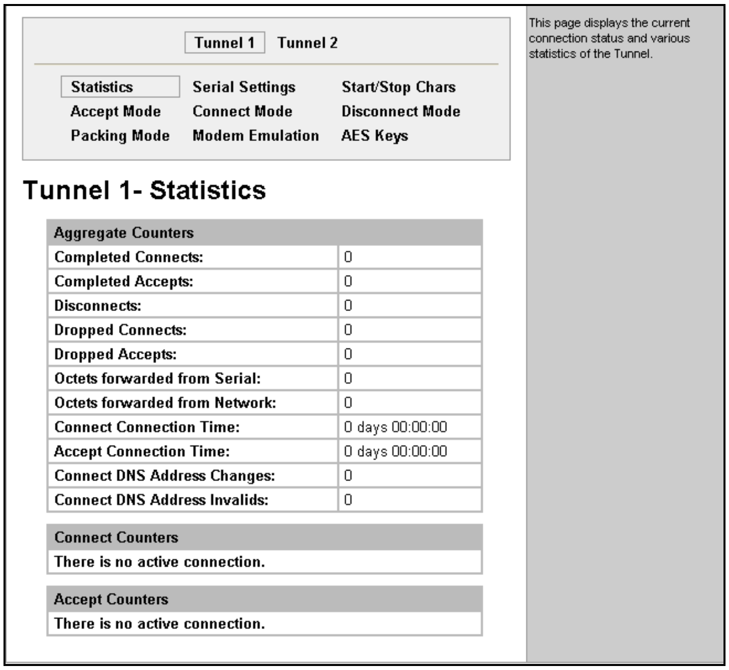
The Tunnel pages allow you to view current statistics and configure serial settings, Connect Mode, Accept Mode, Disconnect Mode, Packing Mode, start and stop characters, modem emulation, and AES keys.

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 4-7. Tunnel 1



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

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.

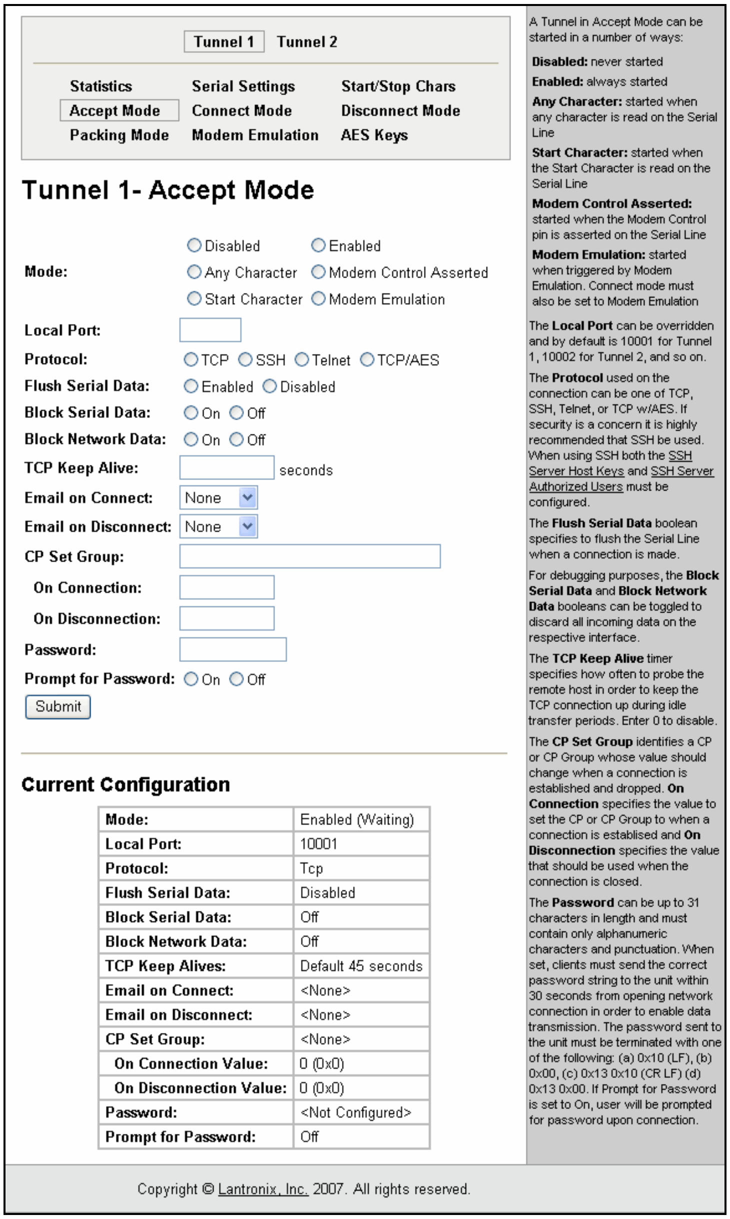
Accept Mode

In Accept Mode, the MatchPort AR 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 4-8. Tunnel 1 Accept Mode



Tunnel 1- Accept Mode

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

Local Port:

Protocol: ○ TCP ○ SSH ○ Telnet ○ TCP/AES

Flush Serial Data: ○ Enabled ○ Disabled

Block Serial Data: ○ On ○ Off

Block Network Data: ○ On ○ Off

TCP Keep Alive: seconds

Email on Connect: None

Email on Disconnect: None

CP Set Group:

On Connection:

On Disconnection:

Password:

Prompt for Password: ○ On ○ Off

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

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 establised 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.

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

2. Enter or modify the following settings:

Tunnel - Accept Mode Page Settings	Description
Mode	Select the method used to start a tunnel in Accept mode. Choices are: **Disabled** = do not accept an incoming connection. **Enabled** = accept an incoming connection. (*default*) **Any Character** = start waiting for an incoming connection when any character is read on the serial line. **Start Character** = start waiting for an incoming connection when the start character for the selected tunnel is read on the serial line. **Modem Control Asserted** = start waiting for an incoming connection as long as the Modem Control pin (DSR) is asserted on the serial line until a connection is made. **Modem Emulation** = start waiting for an incoming connection when triggered by modem emulation AT commands. Connect mode must also be set to **Modem Emulation.**
Local Port	Enter the port number for use as the local port. The defaults are port **10001** for Tunnel 1 and port **10002** for Tunnel 2.
Protocol	Select the protocol type for use with Accept Mode. The default protocol is **TCP**.
Flush Serial Data	Select **Enabled** to flush the serial data buffer on a new connection.
Block Serial Data	Select **On** to block, or not tunnel, serial data transmitted to the MatchPort AR.
Block Network Data	Select **On** to block, or not tunnel, network data transmitted to the MatchPort AR.
TCP Keep Alive	Enter the time, in milliseconds, the MatchPort AR waits during a silent connection before checking if the currently connected network device is still on the network. If the unit then gets no response after 8 attempts, it drops that connection.
Email on Connect	Select whether the MatchPort AR sends an email when a connection is made. Select **None** if you do not want to send an email. Select **Email #** to send an email corresponding to the tunnel number.
Email on Disconnect	Select MatchPort AR sends an email corresponding to the tunnel number when a connection is closed. Select **None** if you do not want to send an email. Select **Email #** to send an email corresponding to the tunnel number.
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 when a connection is established.
On Disconnection	Specifies the value used when the connection is closed.

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

3. Click **Submit**. Changes are applied immediately to the MatchPort AR.

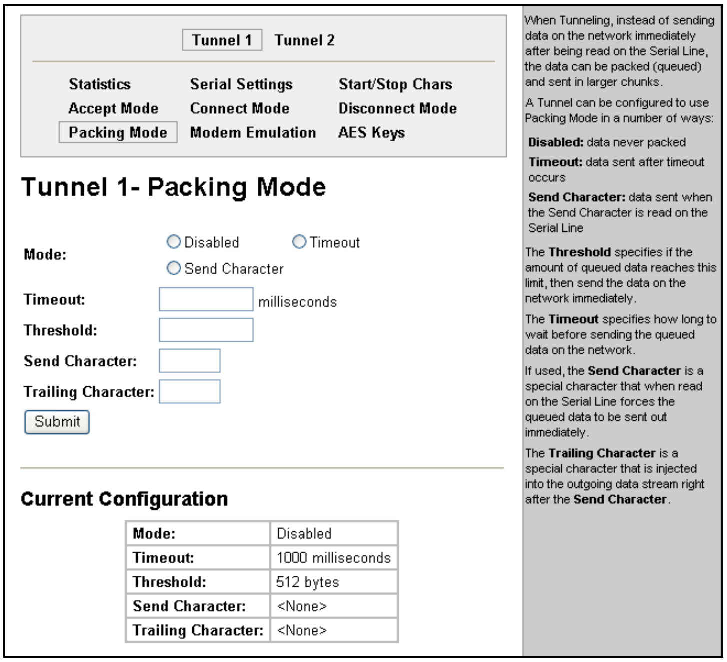
Packing Mode

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:

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

Figure 4-9. Tunnel 1 Packing Mode



Tunnel 1- Packing Mode

Mode: ○ Disabled ○ Timeout ○ Send Character

Timeout: ______ milliseconds

Threshold: ______

Send Character: ______

Trailing Character: ______

Current Configuration

Mode:	Disabled
Timeout:	1000 milliseconds
Threshold:	512 bytes
Send Character:	<None>
Trailing Character:	<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**.

2. Enter or modify the following settings:

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

3. Click **Submit**. Changes are applied immediately to the MatchPort AR.

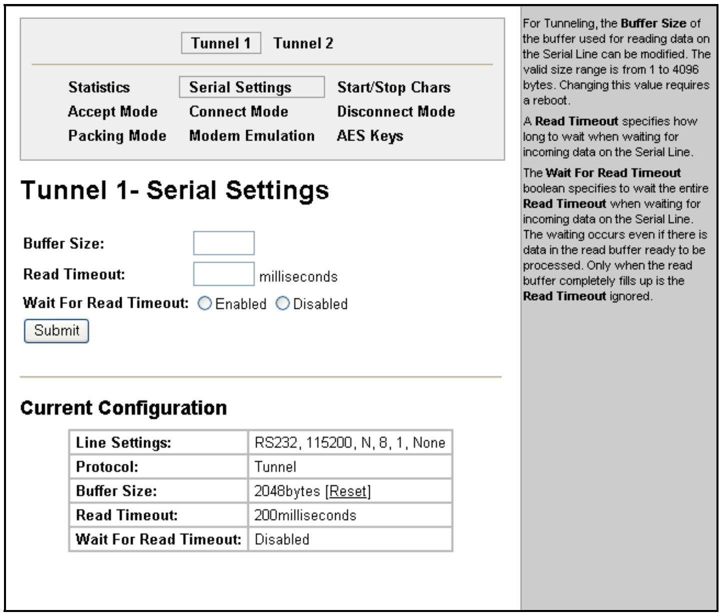
Serial Settings

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:

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

Figure 4-10. Tunnel 1 Serial Settings



Tunnel 1- Serial Settings

Buffer Size:

Read Timeout: milliseconds

Wait For Read Timeout: ○ Enabled ○ Disabled

Current Configuration

Line Settings:	RS232, 115200, N, 8, 1, None
Protocol:	Tunnel
Buffer Size:	2048bytes [Reset]
Read Timeout:	200milliseconds
Wait For Read Timeout:	Disabled

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

A **Read Timeout** specifies how long to wait when waiting for incoming data on the Serial Line.

The **Wait For Read Timeout** boolean specifies to wait the entire **Read Timeout** when waiting for incoming data on the Serial Line. The waiting occurs even if there is data in the read buffer ready to be processed. Only when the read buffer completely fills up is the **Read Timeout** ignored.

2. Enter or modify the following settings:

Tunnel - Serial Settings Page Settings	Description
Buffer Size	Enter the buffer size used for the tunneling of data received. Requires reboot to take effect.
Read Timeout	Enter the time, in milliseconds, for tunneling to wait for serial data.
Wait for Read Timeout	Select **Enabled** to cause the tunneling to wait for a read timeout before forwarding serial data.

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

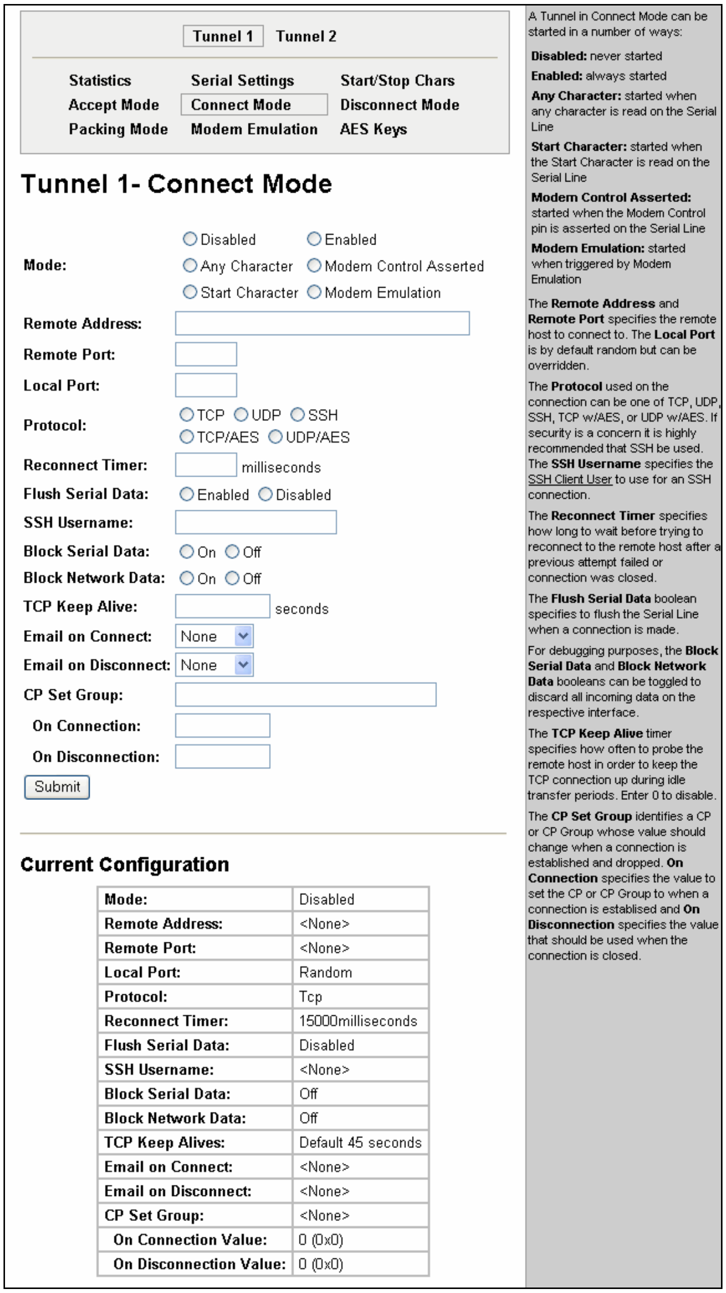
Connect Mode

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 4-11. Tunnel 1 Connect Mode



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:

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 establised 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
Mode	Select the method to be used to attempt a connection to a remote host or device. Choices are: **Disabled** = an outgoing connection is never attempted. (default) **Enabled** = a connection is attempted until one is made. If the connection gets disconnected, the MatchPort AR retries until a connection it makes a connection. **Any Character** = a connection is attempted when any character is read on the serial line. **Modem Control Asserted** = a connection is attempted as long as the Modem Control pin (DSR) is asserted until a connection is made. **Start Character** = a connection is attempted when the start character for the selected tunnel is read on the serial line. **Modem Emulation** = a connection is attempted when triggered by modem emulation AT commands.
Remote Address	Enter the remote address to which the MatchPort AR will connect. Enter an IP address or DNS name.
Remote Port	Enter the remote port number.
Local Port	Enter the port for use as the local port. A random port is selected by default. Once you have configured a number, click the **Random** link in the Current Configuration to switch back to random.
Protocol	Select the protocol type for use in Command Mode. TCP is the default protocol.
Reconnect Timer	Enter the reconnect time in milliseconds. The MatchPort AR attempts to reconnect this amount of time after failing a connection or exiting an existing connection.
Flush Serial Data	Select whether to flush the serial line when a connection is made. Choices are: **Enabled** = flush the serial line when a connection is made. **Disabled** = do not flush the serial line. (default)
SSH Username	Enter the SSH username. The tunnel uses the SSH keys for the client username.
Block Serial Data	Select **On** to block (not tunnel) serial data transmitted to the MatchPort AR.
Block Network Data	Select **On** to block (not tunnel) network data transmitted to the MatchPort AR.
TCP Keep Alive	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.

Tunnel – Connect Mode Page Settings	Description
Email on Connect	Select whether the MatchPort AR sends an email when a connection is made. Select **None** if you do not want to send an email. Select **Email #** to send an email corresponding to the tunnel number.
Email on Disconnect	Select whether the MatchPort AR sends an email corresponding to the tunnel number when a connection is closed. Select **None** if you do not want to send an email. Select **Email #** to send an email corresponding to the tunnel number.
CP Set Group	Identifies a CP or CP Group whose value should change when a connection is established and when it is dropped.
On Connection	Specifies the value to set the CP or CP Group when a connection is established.
On Disconnection	Specifies the value used when the connection is closed.

3. Click **Submit**. Changes are applied immediately to the MatchPort AR.

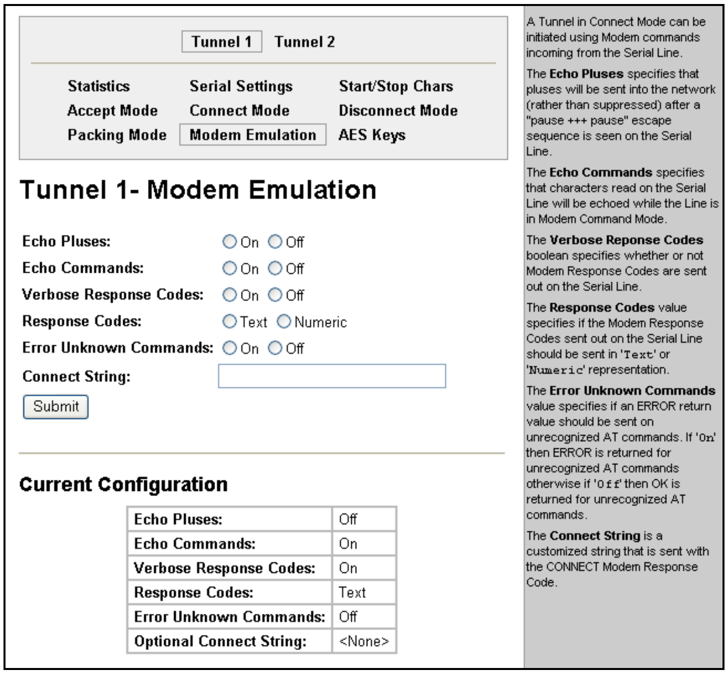
Modem Emulation

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:

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

Figure 4-12. Tunnel 1 Modem Emulation



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 Reponse 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
Echo Pluses	Select **On** to echo **+++** when entering modem Command Mode.
Echo Commands	Select **On** to echo the modem commands to the console.
Verbose Response Codes	Select **On** to send modem response codes out on the serial line.
Response Codes	Select the type of response code from either **Text** or **Numeric**.
Error Unknown Commands	Select whether an **ERROR** or **OK** response is sent in reply to unrecognized AT commands. Choices are: **On** = **ERROR** is returned for unrecognized AT commands. **Off** = **OK** is returned for unrecognized AT commands. (default)
Connect String	Enter the connect string. This modem initialization string prepares the modem for communications. It is a customized string sent with the “CONNECT” modem response code.

3. Click **Submit**. Changes are applied immediately to the MatchPort AR.

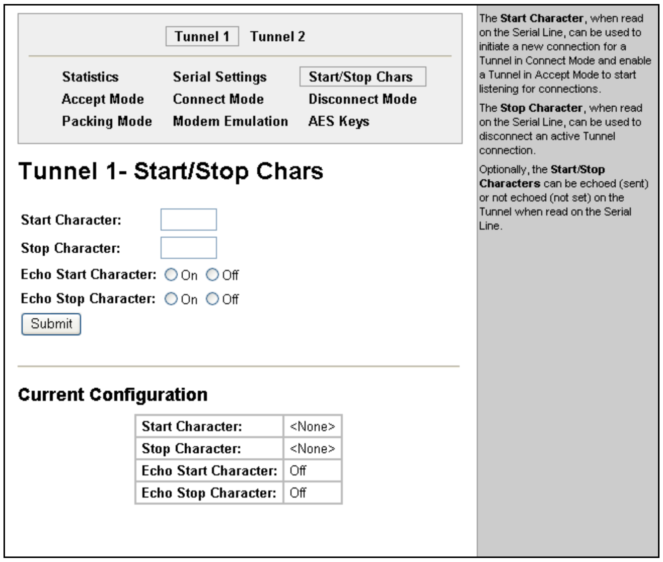
Start and Stop Characters

The Start/Stop Chars page enables you to configure the MatchPort AR 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 4-13. Tunnel 1 Start/Stop Chars



Tunnel 1- Start/Stop Chars

Start Character:

Stop Character:

Echo Start Character: ○ On ○ Off

Echo Stop Character: ○ On ○ Off

Current Configuration

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

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

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

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

2. Enter or modify the following settings:

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

3. Click **Submit**. Changes are applied immediately to the MatchPort AR.

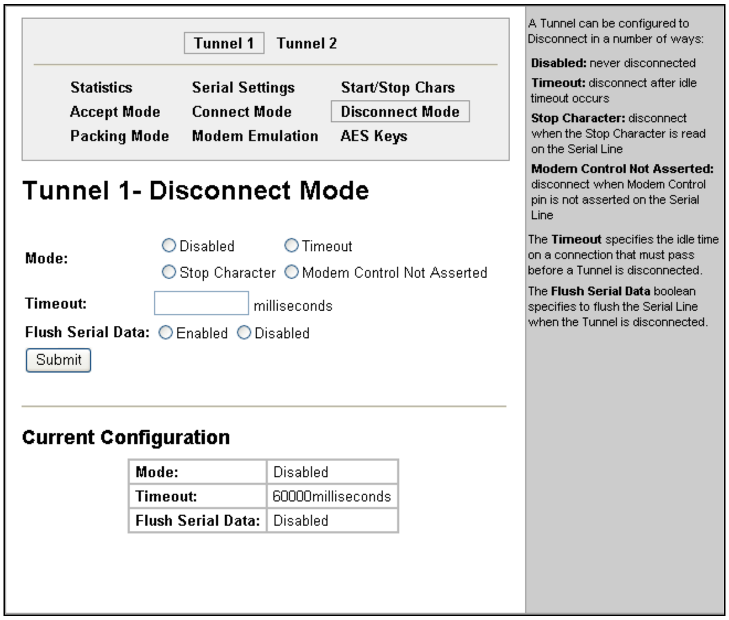
Disconnect Mode

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 4-14. Tunnel 1 Disconnect Mode



Tunnel 1- Disconnect Mode

Mode: ○ Disabled ○ Timeout ○ Stop Character ○ Modem Control Not Asserted

Timeout: ______ milliseconds

Flush Serial Data: ○ Enabled ○ Disabled

Current Configuration

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

A Tunnel can be configured to Disconnect in a number of ways:

Disabled: never disconnected

Timeout: disconnect after idle timeout occurs

Stop Character: disconnect when the Stop Character is read on the Serial Line

Modem Control Not Asserted: disconnect when Modem Control pin is not asserted on the Serial Line

The **Timeout** specifies the idle time on a connection that must pass before a Tunnel is disconnected.

The **Flush Serial Data** boolean specifies to flush the Serial Line when the Tunnel is disconnected.

2. Enter or modify the following settings:

Tunnel – Disconnect Mode Page Settings	Description
Mode	Select the method to use to disconnect from a remote host or device. Choices are: **Disabled** = disable Disconnect Mode completely.

Tunnel – Disconnect Mode Page Settings	Description
	Timeout = enable disconnecting upon the timeout. **Stop Character** =enable disconnecting upon receiving the stop character. **Modem Control Not Asserted** = disconnect an active connection when the Modem Control pin (DSR) is de-asserted on the serial line.
Timeout	Enter a time, in milliseconds, for the MatchPort AR to disconnect on a timeout (if specified as the **Mode**).
Flush Serial Data	Select **Enabled** to flush the serial data buffer on a disconnection.

3. Click **Submit**. Changes are applied immediately to the MatchPort AR.

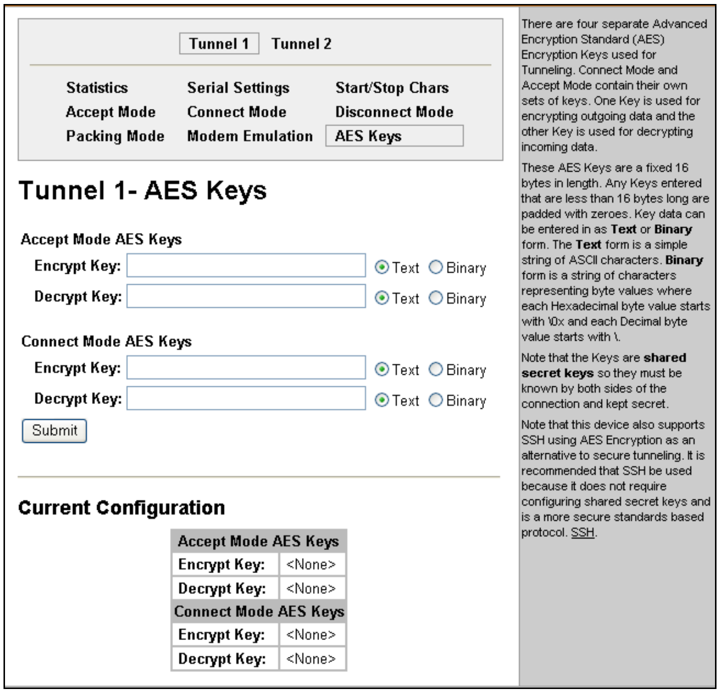
AES Keys

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 4-15. 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.

2. Enter or modify the following settings:

Tunnel – AES Keys Page Settings	Description
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 byes 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**.*

3. Click **Submit**. Changes are applied immediately to the MatchPort AR.

Configurable Pin Manager

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

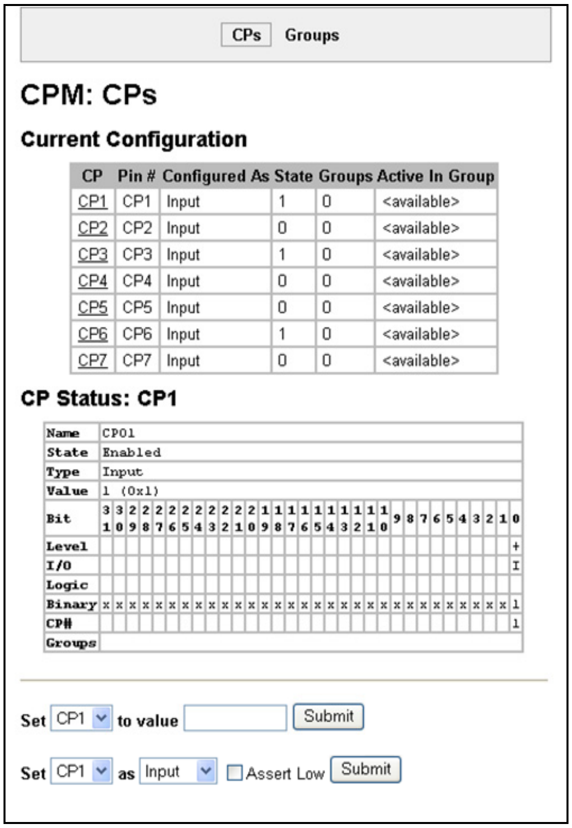
CPM: Configurable Pins

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 AR's CPs:

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

Figure 4-16. CPM: CPs



CPM: CPs

Current Configuration

CP	Pin #	Configured As	State	Groups	Active In Group
CP1	CP1	Input	1	0	<available>
CP2	CP2	Input	0	0	<available>
CP3	CP3	Input	1	0	<available>
CP4	CP4	Input	0	0	<available>
CP5	CP5	Input	0	0	<available>
CP6	CP6	Input	1	0	<available>
CP7	CP7	Input	0	0	<available>

CP Status: CP1

Name	CP01																															
State	Enabled																															
Type	Input																															
Value	1 (0x1)																															
Bit	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
Level																																+
I/O																																I
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	1
CP#																																1
Groups																																

Set CP1 to value Submit

Set CP1 as Input □ Assert Low Submit

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 **Input** is set to read input. A CP configured as **Output** drives data out of the MatchPort AR.
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
Name	Displays the CP number.
State	Displays the current enable state of the CP.
Type	Indicates whether the CP is set for input or output.
Value	Displays the last bit in the CP's current value.
Bit	Visual display of the 32 bit placeholders for a CP.
Level	A "**+**" symbol indicates the CP is asserted (the voltage is high). A "**-**"indicates the CP voltage is low.
I/O	Indicates the current status of the pin: **I** = input **O** = output **X** = unassigned
Logic	An "**I**" indicates the CP is inverted.
Binary	Displays the assertion value of the corresponding bit.
CP#	Displays the CP number.
Groups	Lists the groups in which the CP is a member.

Note: *To modify a CP, all groups in which it is a member must be disabled.*

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 AR.

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 AR.

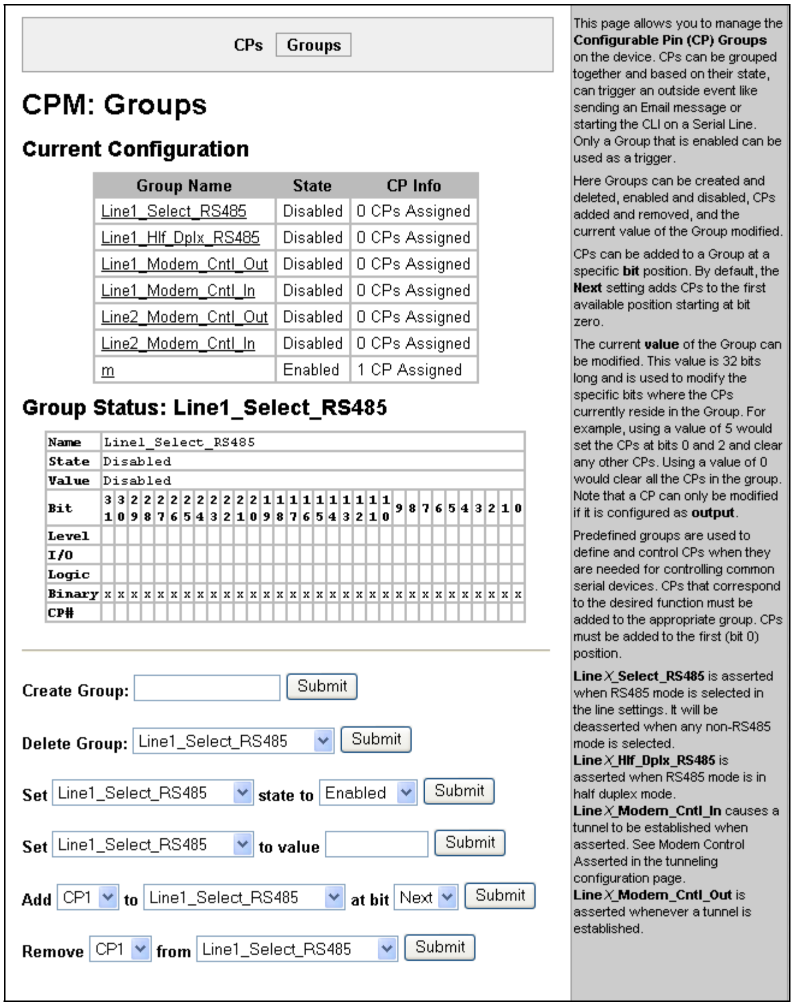
CPM: Groups

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 AR'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 4-17. CPM: Groups



CPM: Groups

Current Configuration

Group Name	State	CP Info
Line1_Select_RS485	Disabled	0 CPs Assigned
Line1_Hlf_Dplx_RS485	Disabled	0 CPs Assigned
Line1_Modem_Cntl_Out	Disabled	0 CPs Assigned
Line1_Modem_Cntl_In	Disabled	0 CPs Assigned
Line2_Modem_Cntl_Out	Disabled	0 CPs Assigned
Line2_Modem_Cntl_In	Disabled	0 CPs Assigned
m	Enabled	1 CP Assigned

Group Status: Line1_Select_RS485

Name	Line1_Select_RS485																															
State	Disabled																															
Value	Disabled																															
Bit	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
Level																																
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
CP#																																

Create Group: [ ] Submit

Delete Group: Line1_Select_RS485 Submit

Set Line1_Select_RS485 state to Enabled Submit

Set Line1_Select_RS485 to value [ ] Submit

Add CP1 to Line1_Select_RS485 at bit Next Submit

Remove CP1 from Line1_Select_RS485 Submit

This page allows you to manage the **Configurable Pin (CP) Groups** 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. Only a Group that is enabled can be used as a trigger.

Here Groups can be created and deleted, enabled and disabled, CPs added and removed, and the current value of the Group modified.

CPs can be added to a Group at a specific **bit** position. By default, the **Next** setting adds CPs to the first available position starting at bit zero.

The current **value** of the Group can be modified. This value is 32 bits long and is used to modify the specific bits where the CPs currently reside in the Group. For example, using a value of 5 would set the CPs at bits 0 and 2 and clear any other CPs. Using a value of 0 would clear all the CPs in the group. Note that a CP can only be modified if it is configured as **output**.

Predefined groups are used to define and control CPs when they are needed for controlling common serial devices. CPs that correspond to the desired function must be added to the appropriate group. CPs must be added to the first (bit 0) position.

Line*X***_Select_RS485** is asserted when RS485 mode is selected in the line settings. It will be deasserted when any non-RS485 mode is selected.
Line*X***_Hlf_Dplx_RS485** is asserted when RS485 mode is in half duplex mode.
Line*X***_Modem_Cntl_In** causes a tunnel to be established when asserted. See Modem Control Asserted in the tunneling configuration page.
Line*X***_Modem_Cntl_Out** is asserted whenever a tunnel is established.

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

Current Configuration

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

3. 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
Name	Displays the CP Group name.
State	Current enable state of the CP group.
Value	Displays the CP group's current value.
Bit	Visual display of the 32 bit placeholders for a CP.
Level	A "**+**" symbol indicates the CP's bit position is asserted (the voltage is high). A "**-**"indicates the CP voltage is low.
I/O	Indicates the current status of the pin: **I** = input **O** = output **X** = unassigned
Logic	An "**I**" indicates the CP is inverted.
Binary	Displays the assertion value of the corresponding bit.
CP#	Displays the configurable pin number and its bit position in the CP group.

To create a CP group:

1. Enter a group name in the **Create Group** field.
2. Click **Submit**. Changes are applied immediately to the MatchPort AR.

To delete a CP group:

1. Select the CP group from the **Delete Group** drop-down list.
2. Click **Submit**. Changes are applied immediately to the MatchPort AR.

To enable or disable a CP group:

1. Select the CP group from the **Set** drop-down list.
2. Select the state (**Enabled** or **Disabled**) from the drop-down list.
3. Click **Submit**. Changes are applied immediately to the MatchPort AR.

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 AR.

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 AR.

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 AR.

DNS Configuration

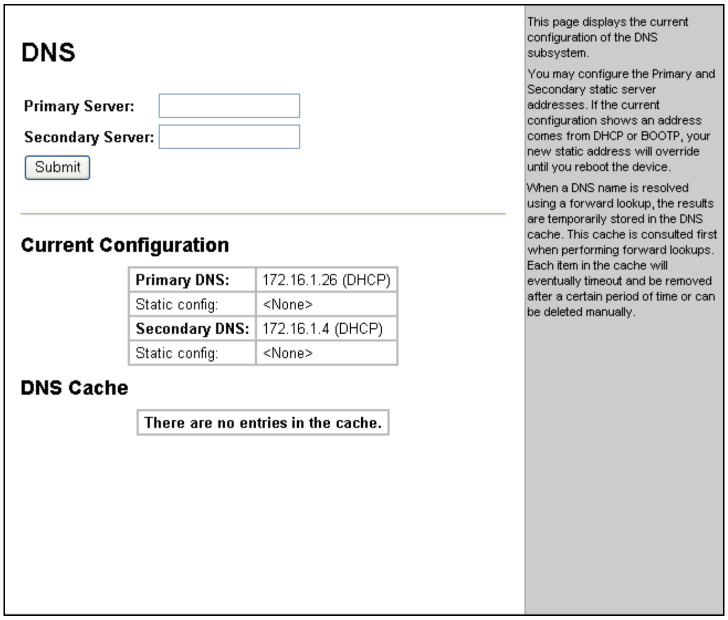
This page displays configuration settings for the domain name system (DNS) and lets you change them as necessary.

The DNS page also shows any contents in the DNS cache. When a DNS name is resolved using a forward lookup, the results are stored in the DNS cache temporarily. The MatchPort AR 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 AR's DNS configuration:

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

Figure 4-18. DNS Settings



DNS

Primary Server:

Secondary Server:

Current Configuration

Primary DNS:	172.16.1.26 (DHCP)
Static config:	<None>
Secondary DNS:	172.16.1.4 (DHCP)
Static config:	<None>

DNS Cache

There are no entries in the cache.

This page displays the current configuration of the DNS subsystem.

You may configure the Primary and Secondary static server addresses. If the current configuration shows an address comes from DHCP or BOOTP, your new static address will override until you reboot the device.

When a DNS name is resolved using a forward lookup, the results are temporarily stored in the DNS cache. This cache is consulted first when performing forward lookups. Each item in the cache will eventually timeout and be removed after a certain period of time or can be deleted manually.

2. Enter or modify the following settings:

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

3. Click **Submit**. Changes are applied immediately to the MatchPort AR.

PPP

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 *5: Point-to-Point Protocol (PPP)*.

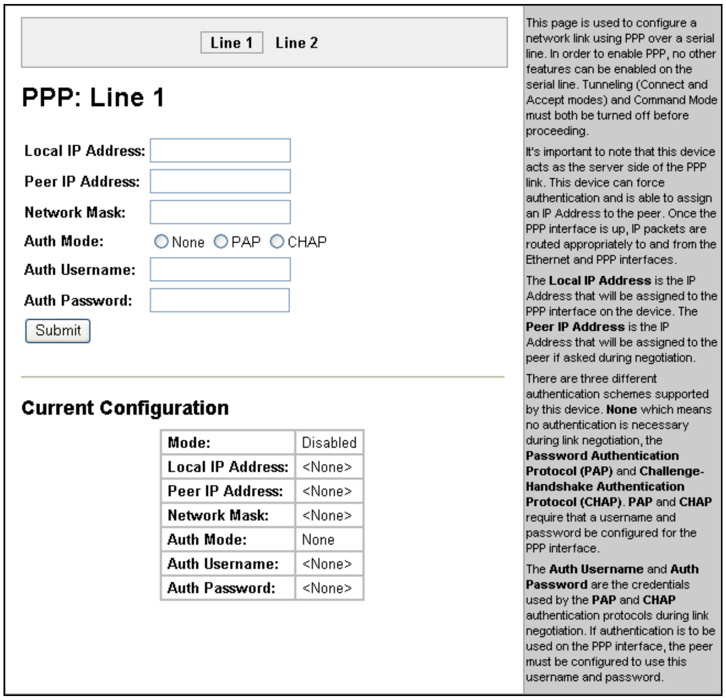
The MatchPort AR supports two types of PPP authorization: Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP). Both of these authentication methods require the configuration of a username and password. The MatchPort AR supports no authentication scheme when no 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.

To configure the MatchPort AR'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 4-19. 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
Local IP Address	Enter the IP address assigned to the MatchPort AR's PPP interface.
Peer IP Address	Enter the IP address assigned to the peer (when requested during negotiation).
Network Mask	Enter the network mask.
Auth. Mode	Choose the authentication mode: **None** = no authentication is required. **PAP** = Password Authentication Protocol. **CHAP** = Challenge Handshake Authentication Protocol.
Auth. Username	Enter the username if authentication is used on the PPP interface.
Auth. Password	Enter the password if authentication is used on the PPP interface.

3. Click **Submit**. Changes are applied immediately to the MatchPort AR

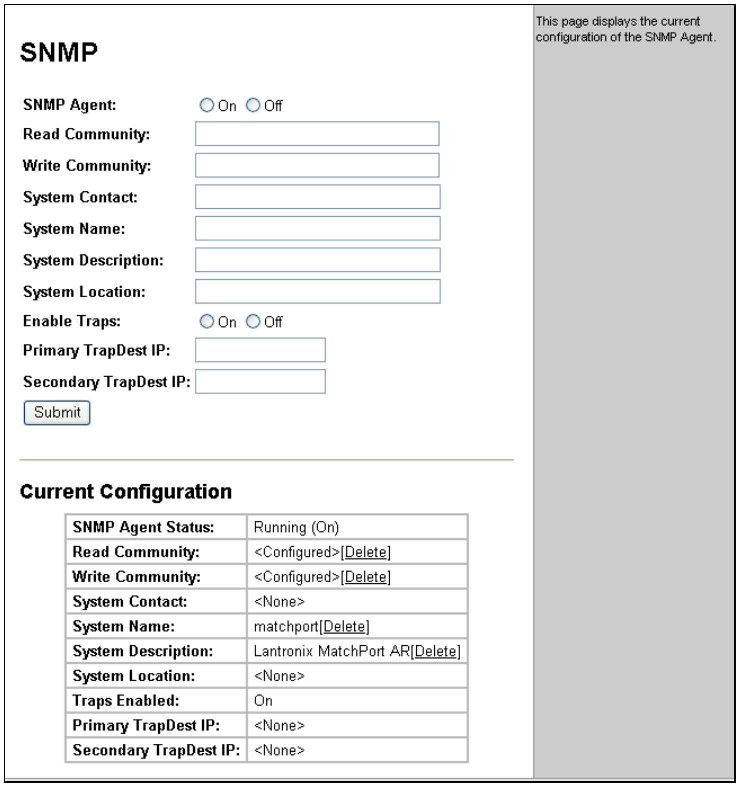
SNMP Configuration

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 4-20. SNMP Configuration



SNMP

SNMP Agent:	○ On ○ Off
Read Community:	
Write Community:	
System Contact:	
System Name:	
System Description:	
System Location:	
Enable Traps:	○ On ○ Off
Primary TrapDest IP:	
Secondary TrapDest IP:	

Current Configuration

SNMP Agent Status:	Running (On)
Read Community:	<Configured>[Delete]
Write Community:	<Configured>[Delete]
System Contact:	<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>

This page displays the current configuration of the SNMP Agent.

2. Enter or modify the following settings:

SNMP Page Settings	Description
SNMP Agent	Select **On** to enable SNMP.
Read Community	Enter the SNMP read-only community string.
Write Community	Enter the SNMP read/write community string.
System Contact	Enter the name of the system contact.
System Name	Enter the system name.
System Description	Enter the system description.
System Location	Enter the system location.

Enable Traps	Select **On** to enable the transmission of the SNMP cold start trap messages. This trap is generated during system boot.
Primary TrapDest IP	Enter the primary SNMP trap host.
Secondary TrapDest IP	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 AR.

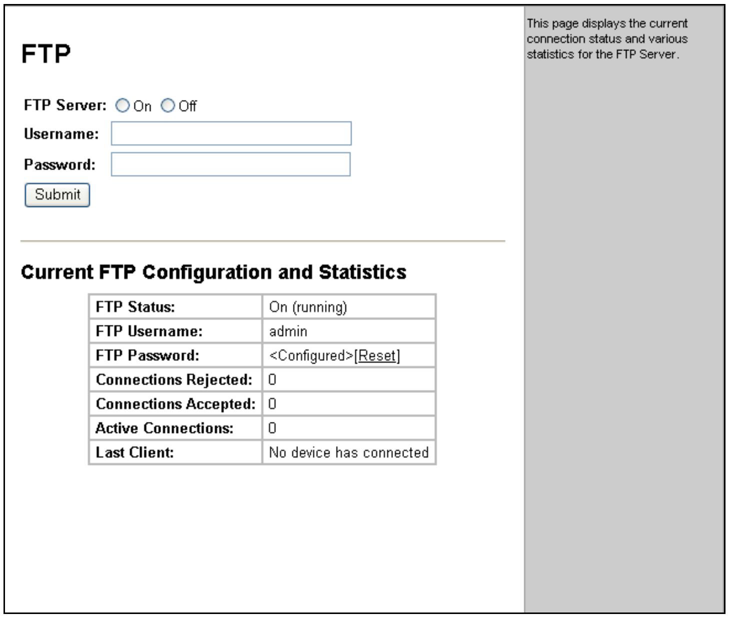
FTP Configuration

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 4-21. FTP Configuration



FTP

FTP Server: ○ On ○ Off

Username:

Password:

Submit

Current FTP Configuration and Statistics

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

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

2. Enter or modify the following settings:

FTP Page Settings	Description
FTP Server	Select **On** to enable the FTP server.
Username	Enter the username to use when logging in via FTP.
Password	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 AR.

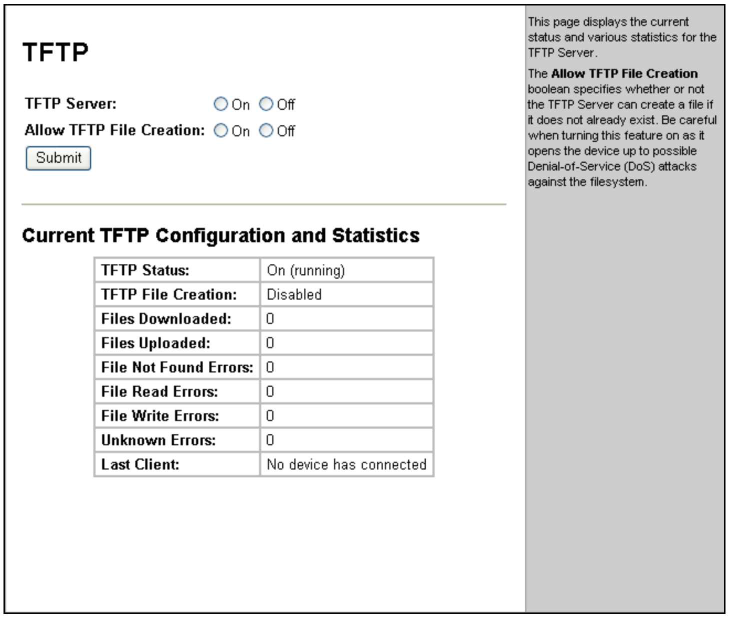
TFTP Configuration

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 4-22. 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
TFTP Server	Select **On** to enable the FTP server.
Allow TFTP File Creation	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 AR.

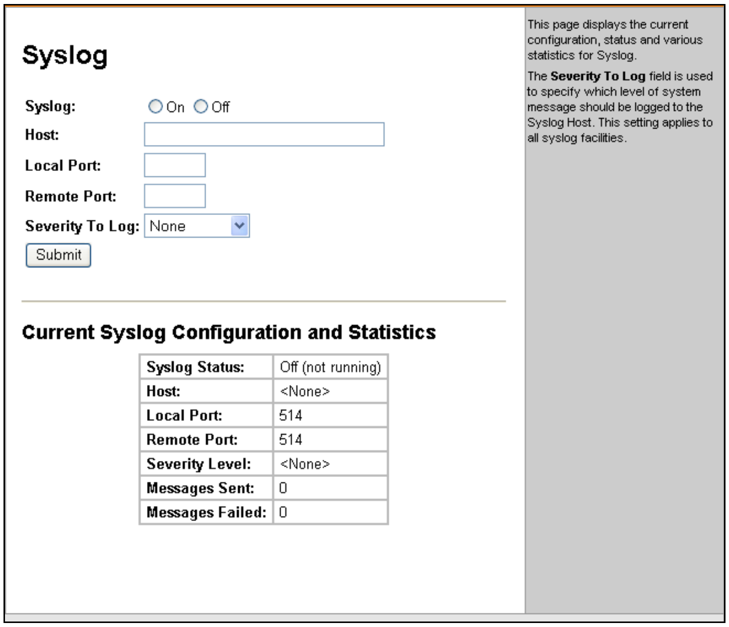
Syslog

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 4-23. 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
Syslog	Select to enable or disable the syslog.
Host	Enter the IP address of the remote server to which system logs are sent for storage.
Local Port	Enter the number of the local port on the MatchPort AR to which system logs are sent.
Remote Port	Enter the number of the port on the remote server that supports logging services. The default is **514**.
Severity to Log	From the drop-down box, select the minimum level of system message the MatchPort AR should log. This setting applies to all syslog facilities. The drop-down list is in descending order of severity (e.g., **Emergency** is more severe than **Alert.**)

HTTP Settings

Hypertext Transfer Protocol (HTTP) is the transport protocol for communicating hypertext documents on the Internet. HTTP defines how messages are formatted and transmitted. It also defines the actions Web servers and browsers should take in response to different commands. This page has three links at the top for viewing statistics and for viewing and changing configuration and authentication settings.

HTTP Statistics

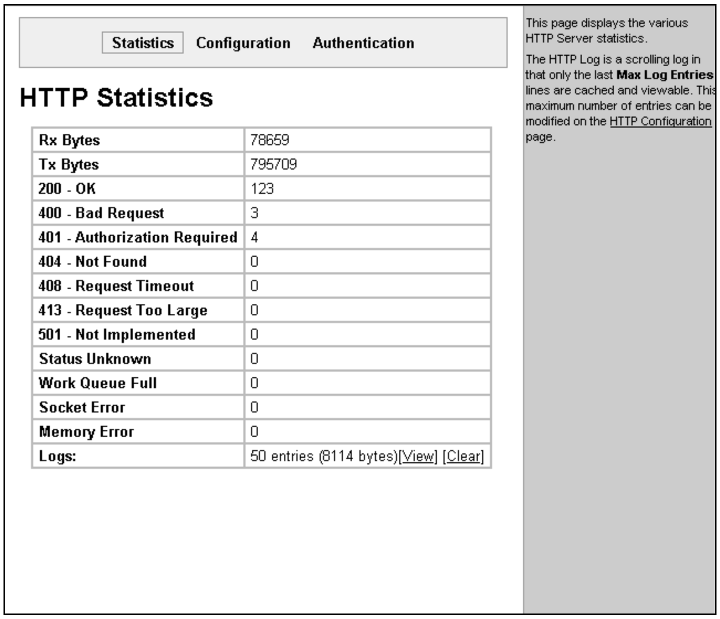
Note: The HTTP log is a scrolling log, with the last Max Log Entries cached and viewable. You can change the maximum number of entries that can be viewed on the HTTP Configuration Page.

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 4-24. HTTP Statistics



HTTP Statistics

Rx Bytes	78659
Tx Bytes	795709
200 - OK	123
400 - Bad Request	3
401 - Authorization Required	4
404 - Not Found	0
408 - Request Timeout	0
413 - Request Too Large	0
501 - Not Implemented	0
Status Unknown	0
Work Queue Full	0
Socket Error	0
Memory Error	0
Logs:	50 entries (8114 bytes)[View] [Clear]

This page displays the various HTTP Server statistics.

The HTTP Log is a scrolling log in that only the last **Max Log Entries** lines are cached and viewable. This maximum number of entries can be modified on the HTTP Configuration page.

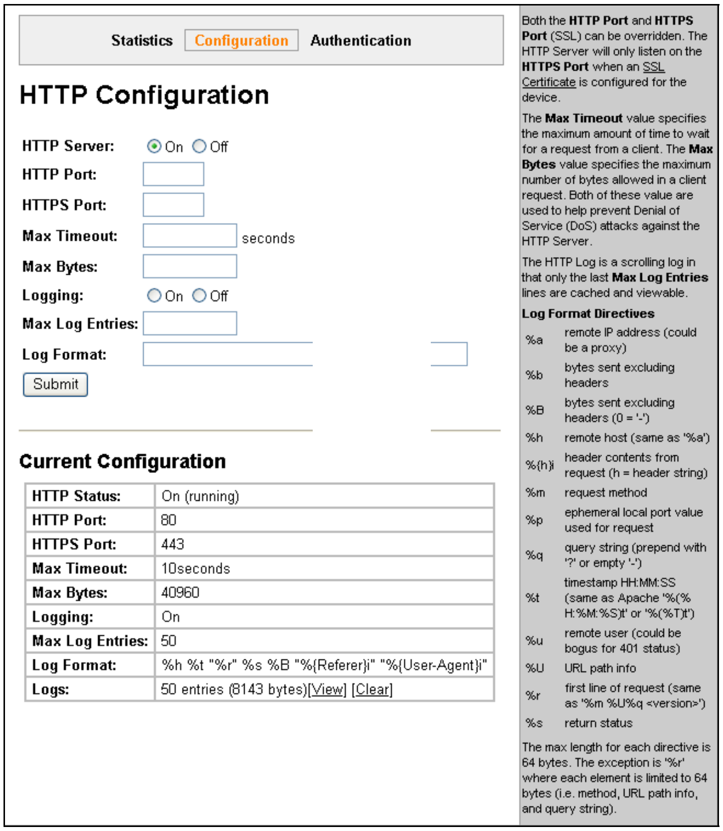
HTTP Configuration

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 4-25. HTTP Configuration



HTTP Configuration

HTTP Server:	● On ○ Off
HTTP Port:	
HTTPS Port:	
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
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 (8143 bytes)[View] [Clear]

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

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

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

Log Format Directives

%a	remote IP address (could be a proxy)
%b	bytes sent excluding headers
%B	bytes sent excluding headers (0 = '-')
%h	remote host (same as '%a')
%{h}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 **On** to enable the HTTP server.
HTTP Port	Enter the port for the HTTP server to use. The default is **80**.
HTTPS Port	Enter the port for the HTTPS server to use. The default is **443**. The HTTP server only listens on the **HTTPS Port** when an SSL certificate is configured.
Max Timeout	Enter the maximum time for the HTTP server to wait when receiving a request. This prevents Denial-of-Service (DoS) attacks. The default is **10** seconds.
Max Bytes	Enter the maximum number of bytes the HTTP server accepts when receiving a request. The default is **40** KB (this prevents DoS attacks).

HTTP Configuration Page Settings	Description
Logging	Select **On** to enable HTTP server logging.
Max Log Entries	Sets the maximum number of HTTP server log entries. Only the last **Max Log Entries** are cached and viewable.
Log Format	Set the log format string for the HTTP server. The **Log Format** directives are as follows: **%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

2. Click **Submit**. Changes are applied immediately to the MatchPort AR.

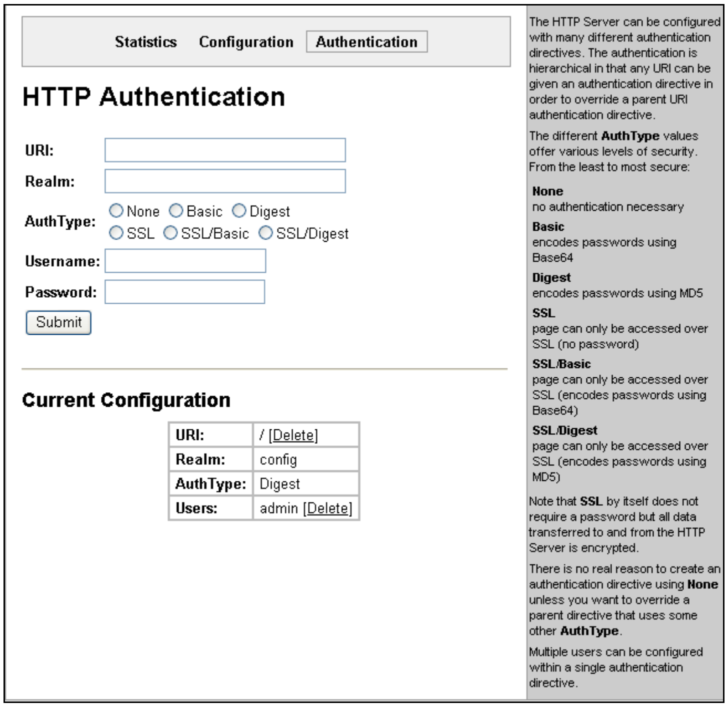
HTTP Authentication

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

To configure HTTP authentication settings:

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

Figure 4-26. HTTP Authentication



HTTP Authentication

URI:

Realm:

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

Username:

Password:

Submit

Current Configuration

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

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

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

None
no authentication necessary

Basic
encodes passwords using Base64

Digest
encodes passwords using MD5

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

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

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

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

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

Multiple users can be configured within a single authentication directive.

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	Select the authentication type: **None** = no authentication is necessary. **Basic** = encodes passwords using Base64. **Digest** = encodes passwords using MD5. **SSL** = the page can only be accessed over SSL (no password is required). **SSL/Basic** = the page is accessible only over SSL and encodes passwords using Base64. **SSL/Digest** = the page is accessible only over SSL and encodes passwords using MD5.
Username	Enter the **Username** used to access the **URI**.
Password	Enter the **Password** for the **Username**.

3. In the **Current Configuration** table, delete and clear currently stored settings as necessary.

4. Click **Submit**. Changes are applied immediately to the MatchPort AR.

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.*

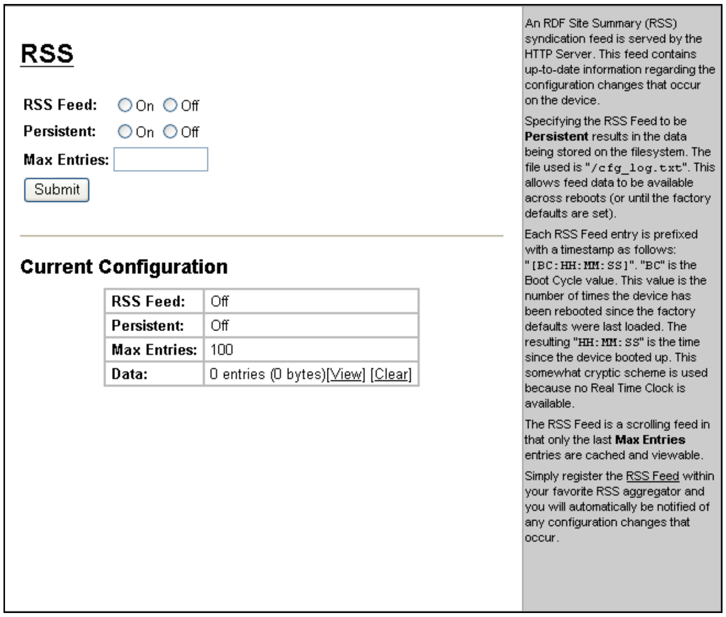
RSS

Really Simple Syndication (RSS) (sometimes referred to as Rich Site Summary) is a method of feeding online content to Web users. Instead of actively searching for MatchPort AR configuration changes, RSS feeds permit viewing only relevant and new information regarding changes made to the MatchPort AR 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 4-27. 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)[View] [Clear]

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

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.

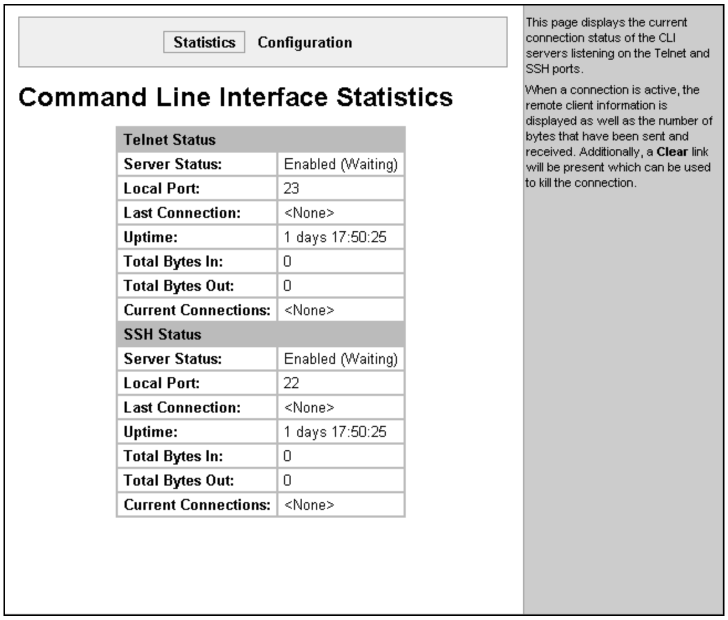
Command Line Interface Statistics

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 4-28. Command Line Interface Statistics



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.

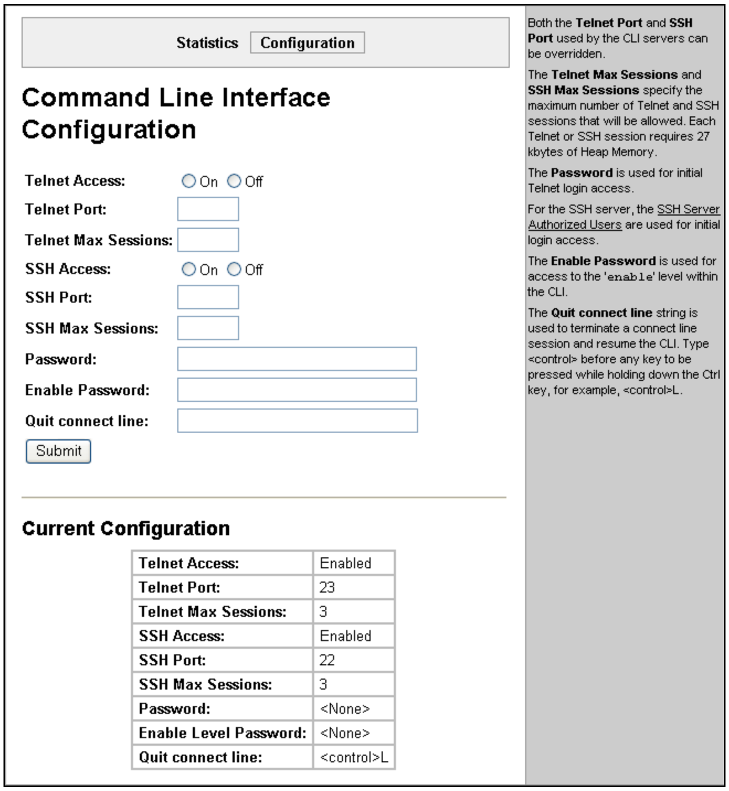
CLI Configuration

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 4-29. Command Line Interface Configuration



Command Line Interface Configuration

Telnet Access:	○ On ○ Off
Telnet Port:	
Telnet Max Sessions:	
SSH Access:	○ On ○ Off
SSH Port:	
SSH Max Sessions:	
Password:	
Enable Password:	
Quit connect line:	

Current Configuration

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

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

The **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 **Password** is used for initial Telnet login access.

For the SSH server, the SSH Server Authorized Users are used for initial login access.

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

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

2. Enter or modify the following settings:

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

3. Click **Submit.** Changes are applied immediately to the MatchPort AR.

Email Configuration

The MatchPort AR 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.*

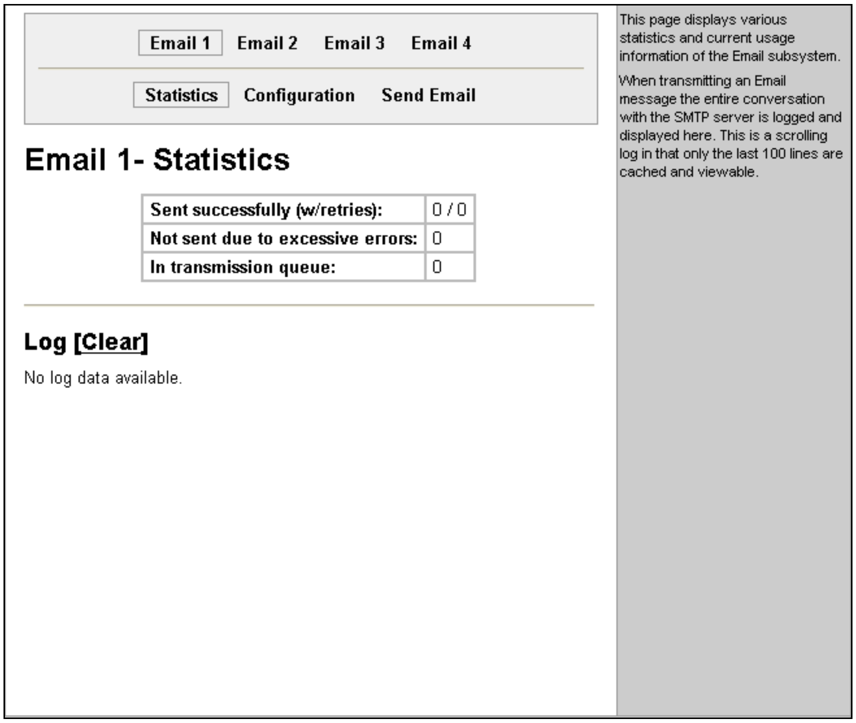
Email Statistics

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 4-30. Email Statistics



Email 1- Statistics

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

Log [Clear]

No log data available.

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

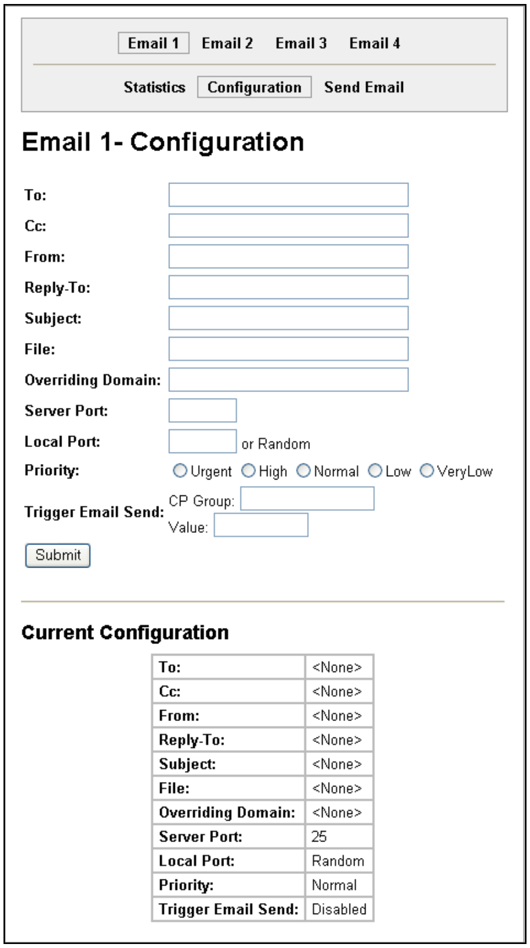
When transmitting an Email message the entire conversation with the SMTP server is logged and displayed here. This is a scrolling log in that only the last 100 lines are cached and viewable.

Email Configuration

To configure MatchPort AR'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 4-31. Email Configuration



Email 1- Configuration

To:	
Cc:	
From:	
Reply-To:	
Subject:	
File:	
Overriding Domain:	
Server Port:	
Local Port:	or Random
Priority:	○ Urgent ○ High ○ Normal ○ Low ○ VeryLow
Trigger Email Send:	CP Group: Value:

Current Configuration

To:	<None>
Cc:	<None>
From:	<None>
Reply-To:	<None>
Subject:	<None>
File:	<None>
Overriding Domain:	<None>
Server Port:	25
Local Port:	Random
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 copied.
From	Enter the email address to list in the From field of the email alert.
Reply-To	Enter the email address to list in the Reply-To field of the email alert.
Subject	Enter the subject for the email alert.
File	Enter the path of the file to send with the email alert. This file displays within the message body of the email.
Overriding Domain	Enter the domain name to override the current domain name in EHLO (Extended Hello).
Server Port	Enter the SMTP server port number. The default is port **25**.

Email – Configuration Page Settings	Description
Local Port	Enter the local port to use for email alerts. The default is a random port number.
Priority	Select the priority level for the email alert.
Trigger Email Send	Configure this field to send an email based on a CP Group trigger. The MatchPort AR sends an email when the specified **Value** matches the current **Group**'s value.

3. In the **Current Configuration** table, delete currently stored settings as necessary.

4. Click **Submit**. Changes are applied immediately to the MatchPort AR.

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.

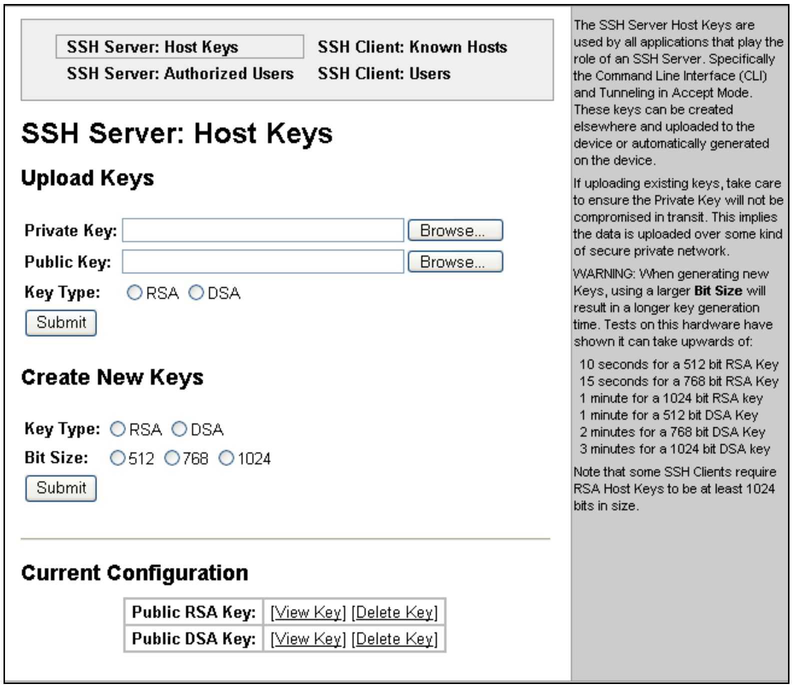
Note: *For more information, see SSH and SSL Security on page 101.*

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 4-32. SSH Server: Host Keys



SSH Server: Host Keys

Upload Keys

Private Key:

Public Key:

Key Type: ○ RSA ○ DSA

Create New Keys

Key Type: ○ RSA ○ DSA

Bit Size: ○ 512 ○ 768 ○ 1024

Current Configuration

Public RSA Key:	[View Key] [Delete Key]
Public DSA Key:	[View Key] [Delete Key]

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
Upload Keys	
Private Key	Enter the path and name of the existing private key you want to upload or use the **Browse** button to select the key. Be sure the private key will not be compromised in transit. This implies the data is uploaded over some kind of secure private network.
Public Key	Enter the path and name of the existing public key you want to upload or use the **Browse** button to select the key.
Key Type	Select a key type to use: **RSA** = use this key with SSH1 and SSH2 protocols. **DSA** = use this key with the SSH2 protocol.
Create New Keys	
Key Type	Select a key type to use for the new key: **RSA** = use this key with the SSH1 and SSH2 protocols. **DSA** = use this key with the SSH2 protocol.
Bit Size	Select a bit length for the new key: **512** **768** **1024**

SSH Server: Host Keys Page Settings	Description
	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 1 minute for a 512 bit DSA Key 2 minutes for a 768 bit DSA Key 3 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 AR.

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 AR 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.

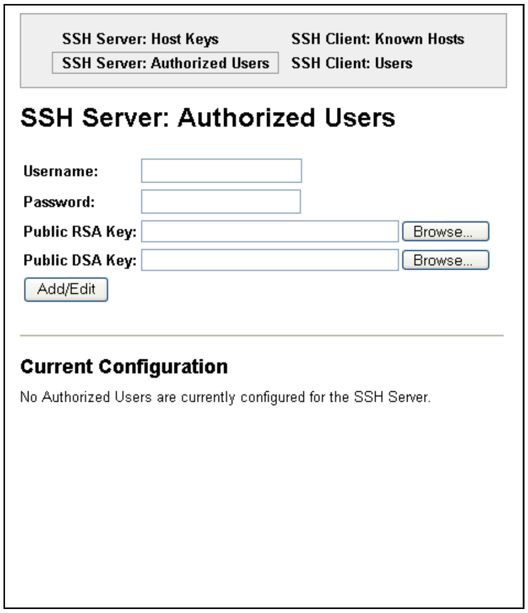
The user's public keys are optional and only necessary if public key authentication is required. Using public key authentication allows a connection to be made without the password being asked.

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 4-33. SSH Server: Authorized Users



SSH Server: Authorized Users

Username:

Password:

Public RSA Key:

Public DSA Key:

Current Configuration

No Authorized Users are currently configured for the SSH Server.

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 **Browse** button to select the key. If authentication is successful with the key, no password is required.
Public DSA Key	Enter the path and name of the existing public DSA key you want to use with this user or use the **Browse** button to select the key. If authentication is successful with the key, no password is required.

3. Click **Submit**. Changes are applied immediately to the MatchPort AR.

SSH Client Known Hosts

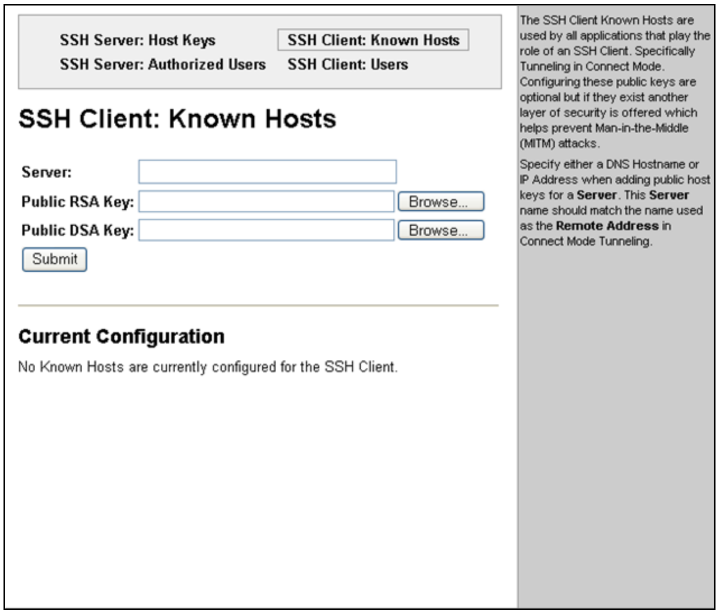
On this page you can change SSH client settings for known hosts.

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 4-34. SSH Client: Known Hosts



SSH Client: Known Hosts

Server:

Public RSA Key:

Public DSA Key:

Current Configuration

No Known Hosts are currently configured for the SSH Client.

The SSH Client Known Hosts are used by all applications that play the role of an SSH Client. Specifically Tunneling in Connect Mode. Configuring these public keys are optional but if they exist another layer of security is offered which helps prevent Man-in-the-Middle (MITM) attacks.

Specify either a DNS Hostname or IP Address when adding public host keys for a **Server**. This **Server** name should match the name used as the **Remote Address** in Connect Mode Tunneling.

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 **Remote Address** in Connect mode tunneling.
Public RSA Key	Enter the path and name of the existing public RSA key you want to use with this known host or use the **Browse** button to select the key.
Public DSA Key	Enter the path and name of the existing public DSA key you want to use with this known host or use the **Browse** button to select the key.

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

3. In the **Current Configuration** table, delete currently stored settings as necessary.

4. Click **Submit**. Changes are applied immediately to the MatchPort AR.

SSH Client User Configuration

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

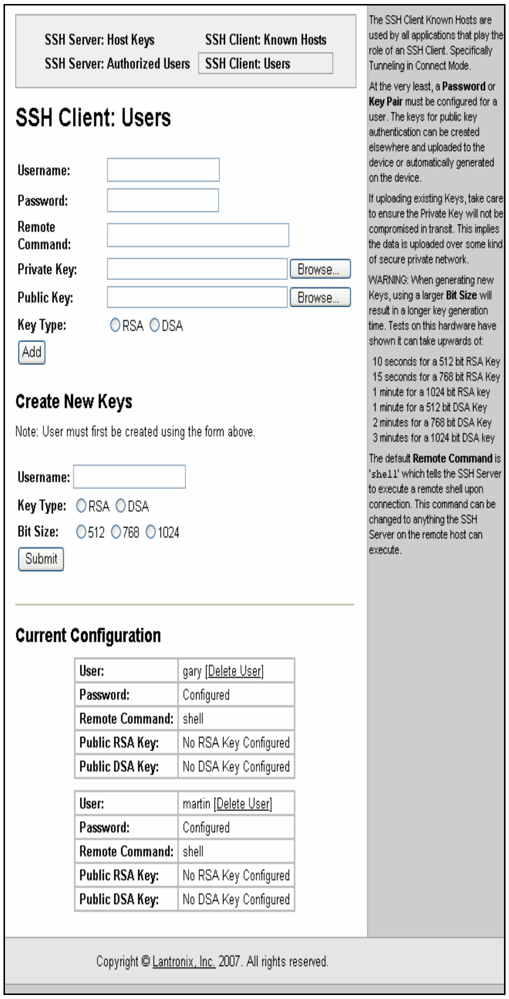
SSH client known hosts are used by all applications that play the role of an SSH client, specifically tunneling in Connect Mode. At the very least, a password or key pair must be configured for a user. The keys for public key authentication can be created elsewhere and uploaded to the device or automatically 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 4-35. SSH Client: Users



SSH Client: Users

Username:

Password:

Remote Command:

Private Key: Browse...

Public Key: Browse...

Key Type: ○ RSA ○ DSA

Add

Create New Keys

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

Username:

Key Type: ○ RSA ○ DSA

Bit Size: ○ 512 ○ 768 ○ 1024

Submit

Current Configuration

User:	gary [Delete User]
Password:	Configured
Remote Command:	shell
Public RSA Key:	No RSA Key Configured
Public DSA Key:	No DSA Key Configured

User:	martin [Delete User]
Password:	Configured
Remote Command:	shell
Public RSA Key:	No RSA Key Configured
Public DSA Key:	No DSA Key Configured

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

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

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

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

10 seconds for a 512 bit RSA Key
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.

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 AR uses to connect to the SSH client user.
Password	Enter the password associated with the username.
Remote Command	Enter the command that can be executed remotely. Default is **shell**, which tells the SSH server to execute a remote shell upon connection. This command can be changed to anything the remote host can perform.
Private Key	Enter the name of the existing private key you want to use with this SSH client user. You can either enter the path and name of the key, or use the **Browse** button to select the key.
Public Key	Enter the path and name of the existing public key you want to use with this SSH client user or use the **Browse** button to select the key.
Key Type	Select the key type to be used. Choices are: **RSA** = use this key with the SSH1 and SSH2 protocols. **DSA** = use this key with the SSH2 protocol.
Create New Keys	
Username	Enter the name of the user associated with the new key.
Key Type	Select the key type to be used for the new key. Choices are: **RSA** = use this key with the SSH1 and SSH2 protocols. **DSA** = use this key with the SSH2 protocol.
Bit Size	Select the bit length of the new key: **512** **768** **1024** Using a larger Bit Size takes more time to generate the key. Approximate times are: 10 seconds for a 512 bit RSA Key 15 seconds for a 768 bit RSA Key 1 minute for a 1024 bit RSA key 1 minute for a 512 bit DSA Key 2 minutes for a 768 bit DSA Key 3 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 AR.

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

5. Click **Submit**. Changes are applied immediately to the MatchPort AR.

SSL Settings

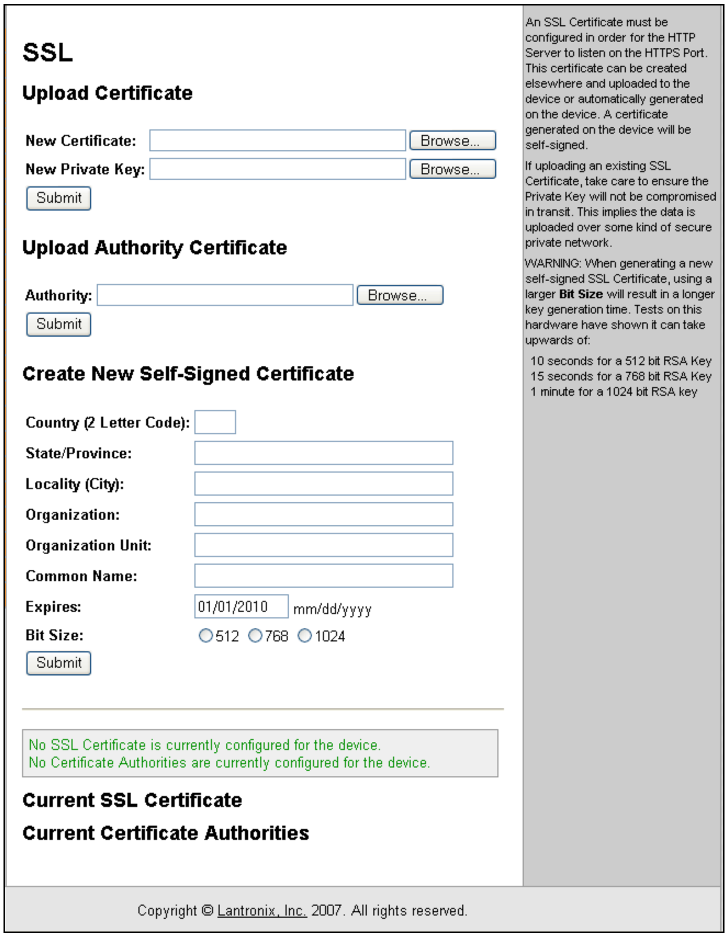
Secure Socket Layer (SSL) is a protocol for managing the security of data transmission over the Internet. It provides encryption, authentication, and message integrity services. SSL is widely used for secure communication to a web server.

The Web Manager also permits the creation of self-signed certificates. This type of SSL certificate is a certificate not signed by a valid Certificate Authority (CA).

To configure the MatchPort AR's SSL settings:

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

Figure 4-36. SSL



SSL

Upload Certificate

New Certificate: Browse...

New Private Key: Browse...

Submit

Upload Authority Certificate

Authority: Browse...

Submit

Create New Self-Signed Certificate

Country (2 Letter Code):

State/Province:

Locality (City):

Organization:

Organization Unit:

Common Name:

Expires: 01/01/2010 mm/dd/yyyy

Bit Size: ○512 ○768 ○1024

Submit

No SSL Certificate is currently configured for the device.
No Certificate Authorities are currently configured for the device.

Current SSL Certificate

Current Certificate Authorities

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

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

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

10 seconds for a 512 bit RSA Key
15 seconds for a 768 bit RSA Key
1 minute for a 1024 bit RSA key

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

2. Enter or modify the following settings:

SSL Page Settings	Description
Upload Certificate	
New Certificate	Enter the path and name of the existing certificate you want to upload, or use the **Browse** button to select the certificate.
New Private Key	Enter the path and name of the existing private key you want to

SSL Page Settings	Description
	upload, or use the **Browse** button to select the private key.
Create New Self-Signed Certificate	
Country (2 Letter Code)	Enter the 2-letter country code to be assigned to the new self-signed certificate. Examples: US for United States and CA for Canada
State/Province	Enter the state or province to be assigned to the new self-signed certificate.
Locality (City)	Enter the city or locality to be assigned to the new self-signed certificate.
Organization	Enter the organization to be associated with the new self-signed certificate. **Example:** If your company is called Widgets, and you are setting up a web server for the Sales department, enter Widgets for the organization.
Organization Unit	Enter the organizational unit to be associated with the new self-signed certificate. **Example:** If your company is setting up a web server for the Sales department, enter Sales for your organizational unit.
Common Name	Enter the same name that the user will enter when requesting your web site. **Example:** If a user enters http://www.widgets.abccompany.com to access your web site, the **Common Name** would be www.widgets.abccompany.com.
Expires	Enter the expiration date, in mm/dd/yyyy format, for the new self-signed certificate. **Example:** An expiration date of May 9, 2007 is entered as 05/09/2007.
Bit Size	Select the bit size of the new self-signed certificate. Choices are: **512** **768** **1024** Using a larger bit size takes more time to generate the key. Approximate times are: 10 seconds for a 512-bit RSA key 15 seconds for a 768-bit RSA key 1 minute for a 1024-bit RSA key

3. Click **Submit**. Changes are applied immediately to the MatchPort AR.

XML Configuration

The MatchPort AR allows for the configuration of units using an XML configuration file. Export a current configuration for use on other MatchPort ARs or import a saved configuration file. For more information on using XML, see *XML* on page 112.

XML Configuration Record: Export System Configuration

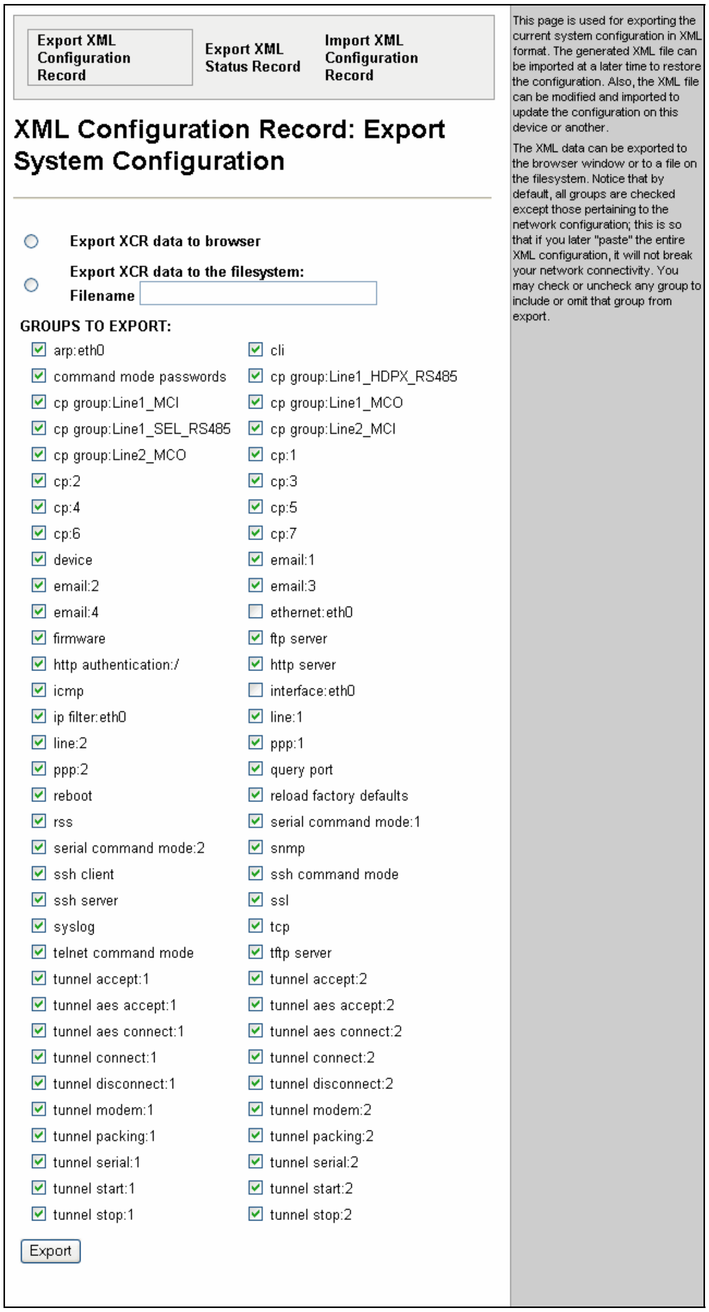
On this page you can export the current system configuration in XML format. The generated XML file can be imported later to restore a configuration. It can also be modified and imported to update the configuration on this MatchPort AR unit or another. The XML data can be exported to the browser window 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:

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

Figure 4-37. XML Configuration Record: Export System Configuration



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

XML Configuration Record: Export System Configuration

○ Export XCR data to browser

○ Export XCR data to the filesystem:
Filename

GROUPS TO EXPORT:

☑ arp:eth0
☑ cli
☑ command mode passwords
☑ cp group:Line1_HDPX_RS485
☑ cp group:Line1_MCI
☑ cp group:Line1_MCO
☑ cp group:Line1_SEL_RS485
☑ cp group:Line2_MCI
☑ cp group:Line2_MCO
☑ cp:1
☑ cp:2
☑ cp:3
☑ cp:4
☑ cp:5
☑ cp:6
☑ cp:7
☑ device
☑ email:1
☑ email:2
☑ email:3
☑ email:4
☐ ethernet:eth0
☑ firmware
☑ ftp server
☑ http authentication:/
☑ http server
☑ icmp
☐ interface:eth0
☑ ip filter:eth0
☑ line:1
☑ line:2
☑ ppp:1
☑ ppp:2
☑ query port
☑ reboot
☑ reload factory defaults
☑ rss
☑ serial command mode:1
☑ serial command mode:2
☑ snmp
☑ ssh client
☑ ssh command mode
☑ ssh server
☑ ssl
☑ syslog
☑ tcp
☑ telnet command mode
☑ tftp server
☑ tunnel accept:1
☑ tunnel accept:2
☑ tunnel aes accept:1
☑ tunnel aes accept:2
☑ tunnel aes connect:1
☑ tunnel aes connect:2
☑ tunnel connect:1
☑ tunnel connect:2
☑ tunnel disconnect:1
☑ tunnel disconnect:2
☑ tunnel modem:1
☑ tunnel modem:2
☑ tunnel packing:1
☑ tunnel packing:2
☑ tunnel serial:1
☑ tunnel serial:2
☑ tunnel start:1
☑ tunnel start:2
☑ tunnel stop:1
☑ tunnel stop:2

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 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.

2. Enter or modify the following settings:

XML Configuration Record: Export System 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.
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.

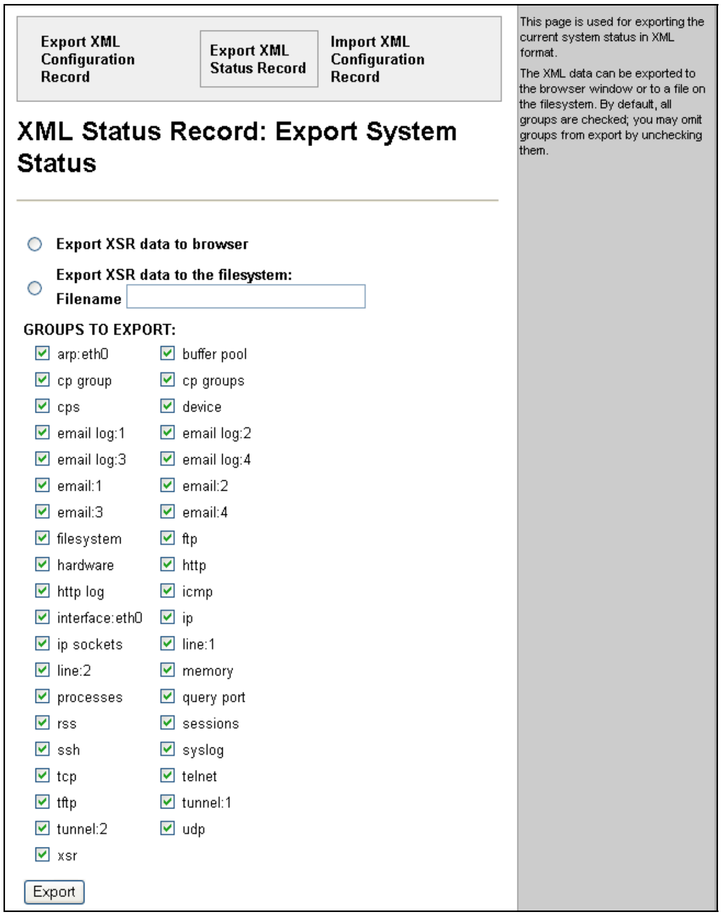
   Note: *To view these files or store them elsewhere, see Filesystem Configuration on page 75.*

XML Status Record: Export System 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 XML Status Record** at the top of the page. The XML Status Record: Export System Status page displays.

Figure 4-38. XML Status Record: Export System Status Page



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

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 are checked; you may omit groups from export by unchecking them.

XML Status Record: Export System Status

○ Export XSR data to browser

○ Export XSR data to the filesystem:
Filename

GROUPS TO EXPORT:

☑ arp:eth0 ☑ buffer pool
☑ cp group ☑ cp groups
☑ cps ☑ device
☑ email log:1 ☑ email log:2
☑ email log:3 ☑ email log:4
☑ email:1 ☑ email:2
☑ email:3 ☑ email:4
☑ filesystem ☑ ftp
☑ hardware ☑ http
☑ http log ☑ icmp
☑ interface:eth0 ☑ ip
☑ ip sockets ☑ line:1
☑ line:2 ☑ memory
☑ processes ☑ query port
☑ rss ☑ sessions
☑ ssh ☑ syslog
☑ tcp ☑ telnet
☑ tftp ☑ tunnel:1
☑ tunnel:2 ☑ udp
☑ xsr

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.
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.

   Note: To view these files or store them elsewhere, see Filesystem Configuration on page 75.

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:

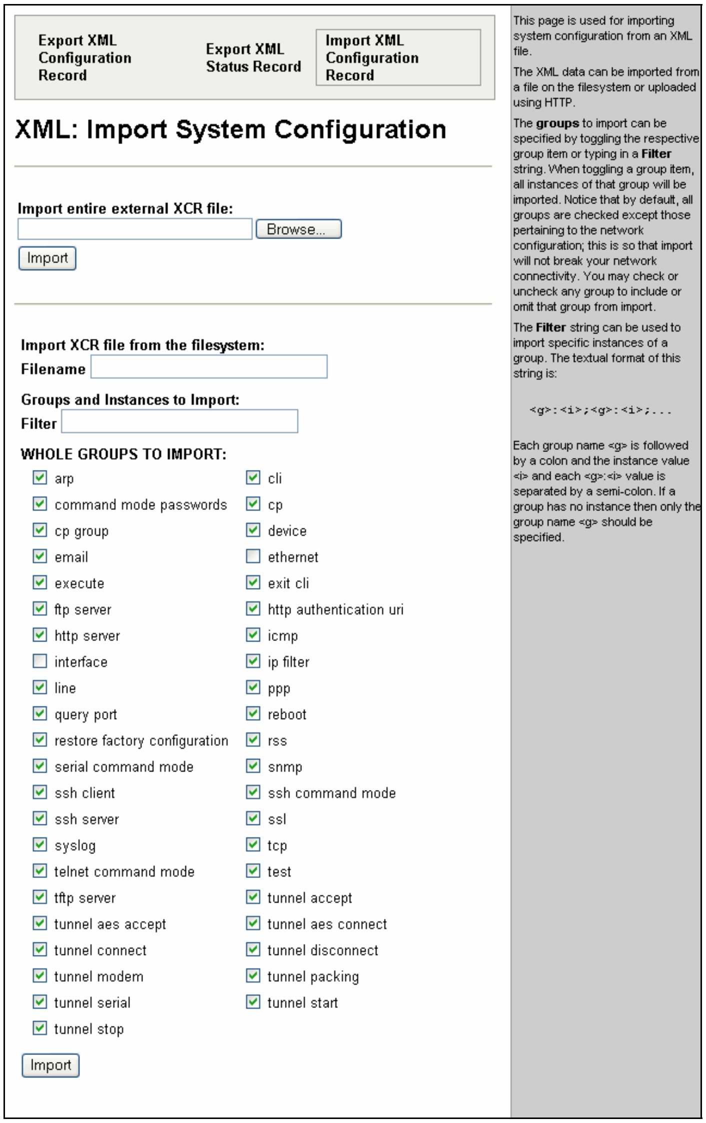
<g>:<i>;<g>:<i>;...

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 XML Configuration Record** at the top of the page. The XML: Import System Configuration page displays.

Figure 4-39. XML: Import System Configuration Page


Export XML Configuration Record
Export XML Status Record
Import XML Configuration Record
Browse...
Import
Import

XML: Import System Configuration

Import entire external XCR file:

Import XCR file from the filesystem:

Filename

Groups and Instances to Import:

Filter

WHOLE GROUPS TO IMPORT:

- ☑ arp
- ☑ cli
- ☑ command mode passwords
- ☑ cp
- ☑ cp group
- ☑ device
- ☑ email
- ☐ ethernet
- ☑ execute
- ☑ exit cli
- ☑ ftp server
- ☑ http authentication uri
- ☑ http server
- ☑ icmp
- ☐ interface
- ☑ ip filter
- ☑ line
- ☑ ppp
- ☑ query port
- ☑ reboot
- ☑ restore factory configuration
- ☑ rss
- ☑ serial command mode
- ☑ snmp
- ☑ ssh client
- ☑ ssh command mode
- ☑ ssh server
- ☑ ssl
- ☑ syslog
- ☑ tcp
- ☑ telnet command mode
- ☑ test
- ☑ tftp server
- ☑ tunnel accept
- ☑ tunnel aes accept
- ☑ tunnel aes connect
- ☑ tunnel connect
- ☑ tunnel disconnect
- ☑ tunnel modem
- ☑ tunnel packing
- ☑ tunnel serial
- ☑ tunnel start
- ☑ tunnel stop

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

The XML data can be imported from a file on the filesystem or uploaded using HTTP.

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

The **Filter** string can be used to import specific instances of a group. The textual format of this string is:

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

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

1. Enter or modify the following settings:

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

2. Click the **Import** button. The settings for the groups selected are applied to the MatchPort AR.

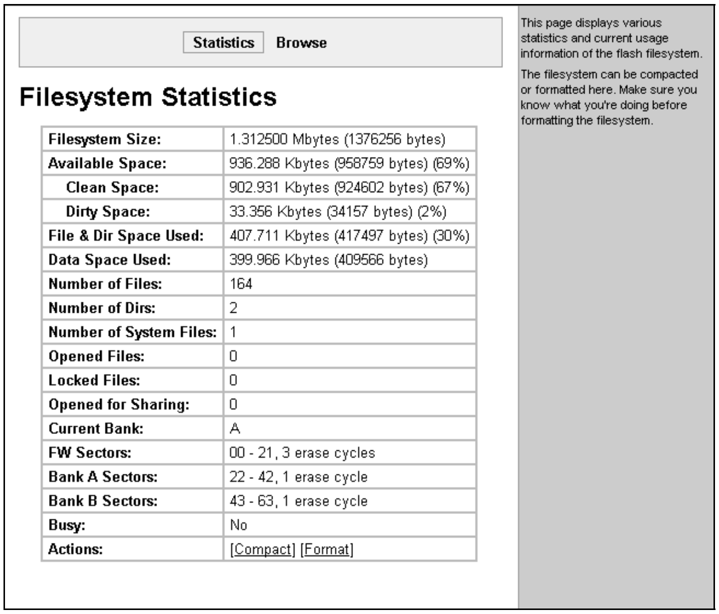
Filesystem Configuration

The MatchPort AR 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 4-40. Filesystem Statistics



Filesystem Statistics

Filesystem Size:	1.312500 Mbytes (1376256 bytes)
Available Space:	936.288 Kbytes (958759 bytes) (69%)
Clean Space:	902.931 Kbytes (924602 bytes) (67%)
Dirty Space:	33.356 Kbytes (34157 bytes) (2%)
File & Dir Space Used:	407.711 Kbytes (417497 bytes) (30%)
Data Space Used:	399.966 Kbytes (409566 bytes)
Number of Files:	164
Number of Dirs:	2
Number of System Files:	1
Opened Files:	0
Locked Files:	0
Opened for Sharing:	0
Current Bank:	A
FW Sectors:	00 - 21, 3 erase cycles
Bank A Sectors:	22 - 42, 1 erase cycle
Bank B Sectors:	43 - 63, 1 erase cycle
Busy:	No
Actions:	[Compact] [Format]

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

The filesystem can be compacted or formatted here. Make sure you know what you're doing before formatting the filesystem.

To view filesystem statistics, compact, or format the MatchPort AR'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**.

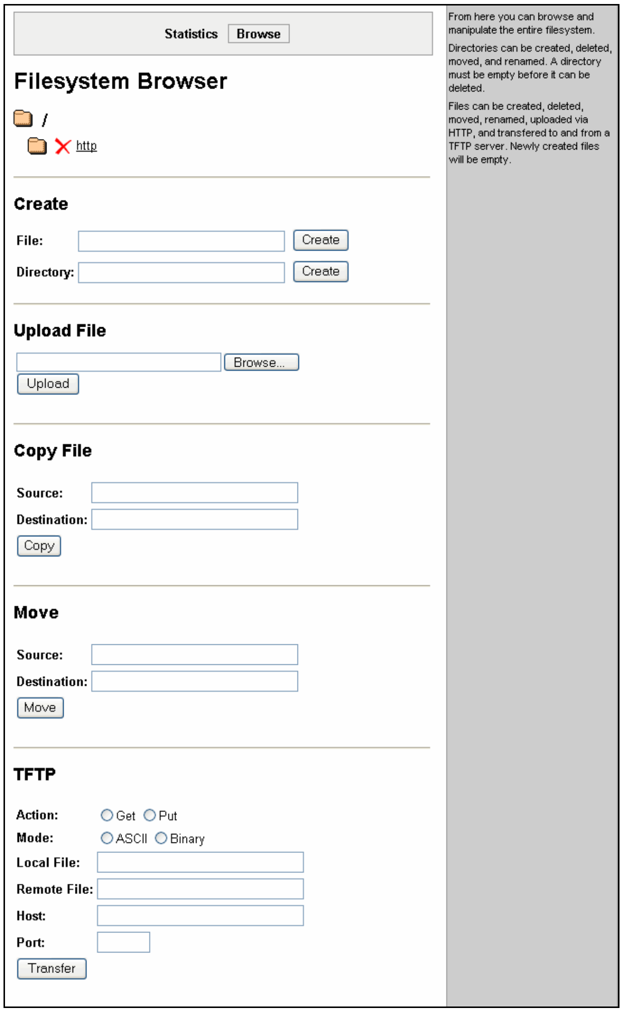
   Note: *All files and configuration settings on the filesystem are destroyed upon formatting, including Web Manager files. Back up all files as necessary. Upon formatting, the current configuration is lost.*

Filesystem Browser

To browse the MatchPort AR'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 4-41. Filesystem Browser



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 transfered 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
Create	
File	Enter the name of the file you want to create, and then click **Create**.
Directory	Enter the name of the directory you want to create, and then click **Create**.
Upload File	Enter the path and name of the file you want to upload by

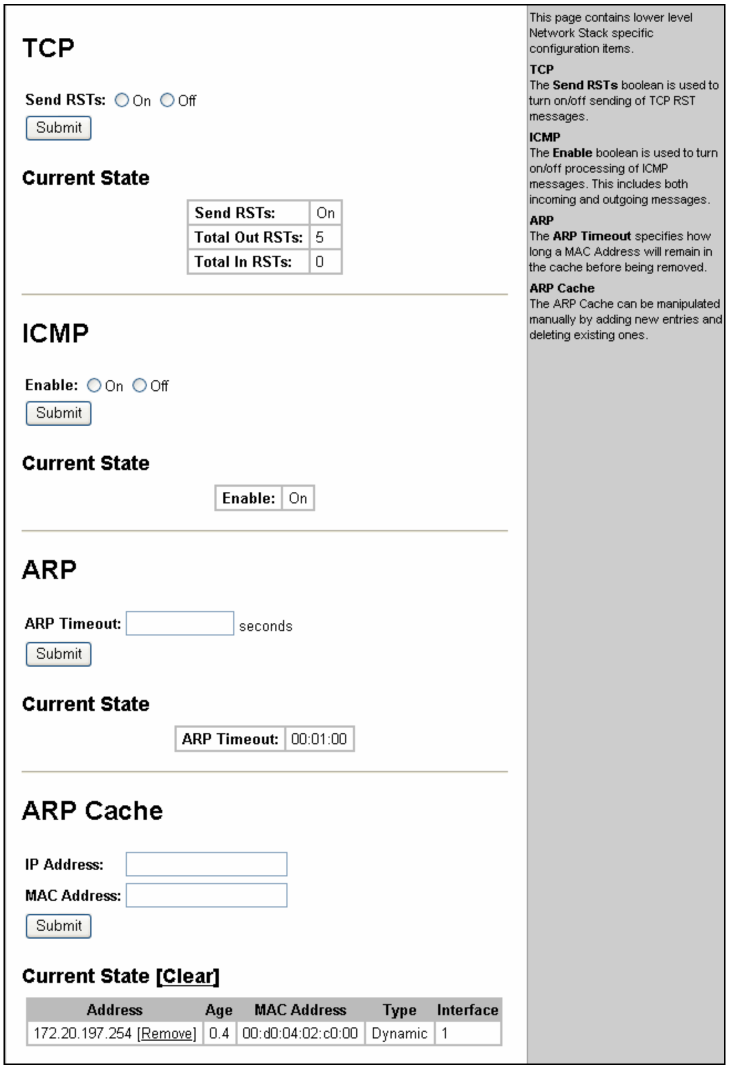
Filesystem Browser Page Settings	Description
	means of HTTP or use the **Browse** button to select the file, and then click **Upload**.
Copy File	
Source	Enter the location where the file you want to copy resides.
Destination	Enter the location where you want the file copied. After you specify a source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

Protocol Stack Configuration

To configure the MatchPort AR'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 4-42. Protocol Stack



TCP

Send RSTs: ○ On ○ Off

Submit

Current State

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

ICMP

Enable: ○ On ○ Off

Submit

Current State

Enable:	On

ARP

ARP Timeout: ______ seconds

Submit

Current State

ARP Timeout:	00:01:00

ARP Cache

IP Address: ______

MAC Address: ______

Submit

Current State [Clear]

Address	Age	MAC Address	Type	Interface
172.20.197.254 [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.

2. Enter or modify the following settings:

Protocol Stack Page Settings	Description
TCP	
Send RSTs	TCP contains six control bits, with one or more defined in each packet. RST is one of the control bits. The RST bit is responsible for telling the receiving TCP stack to end a connection immediately. Sending this flag may pose a security risk. Select **Off** to disable the sending of the RST flag.
ICMP	
Enable	Internet Control Message Protocol (ICMP) can be used as an error-reporting protocol between two hosts. Commands such as `ping` use this protocol. Sending and processing ICMP messages may pose a security risk.
ARP	
ARP Timeout	Enter the time, in milliseconds, for the ARP timeout. This is the maximum duration an address remains in the cache.
ARP Cache	
IP Address	Enter the IP address to add to the ARP table.
MAC Address	Enter the MAC address to add to the ARP table.
Note: Both the IP and MAC addresses are required for the ARP cache.	
Current State	
Clear	Select **Clear** to remove all entries in the ARP table.
Remove	Removes a specific entry from the ARP table.

3. Click **Submit** after each modified field. Changes are applied immediately to the MatchPort AR.

IP Address Filter

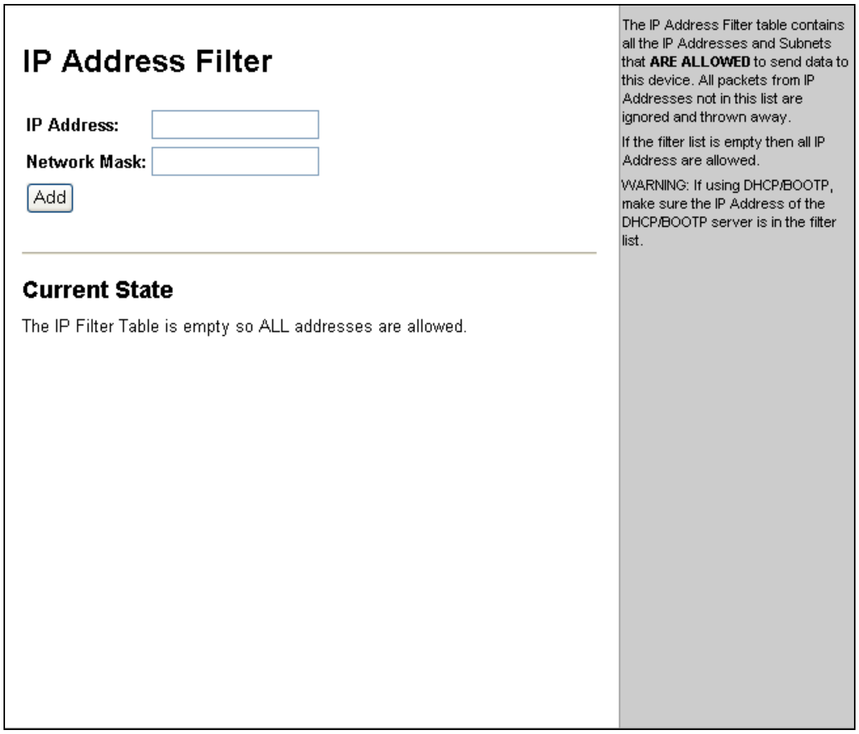
The IP address filter specifies the hosts and subnets permitted to communicate with the MatchPort AR.

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

To configure the IP address filter:

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

Figure 4-43. IP Address Filter Configuration



IP Address Filter

IP Address:

Network Mask:

Current State

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

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.

2. 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.

3. In the **Current State** table, click **Remove** to delete settings as necessary.

4. Click **Submit**. Changes are applied immediately to the MatchPort AR.

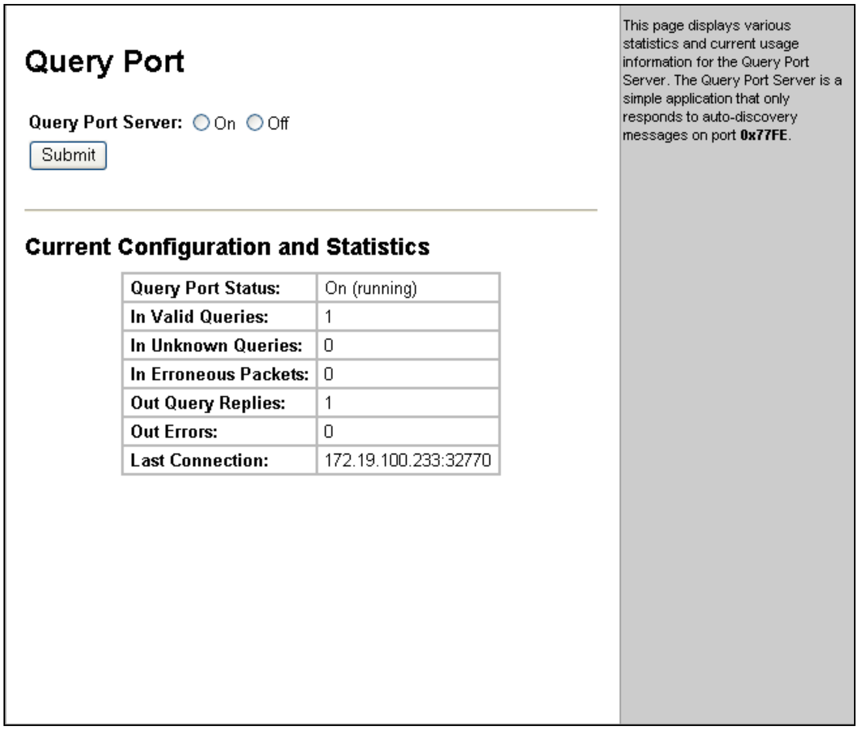
Query Port

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 16.

To configure the query port server:

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

Figure 4-44. 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 AR.

Diagnostics

The MatchPort AR 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.

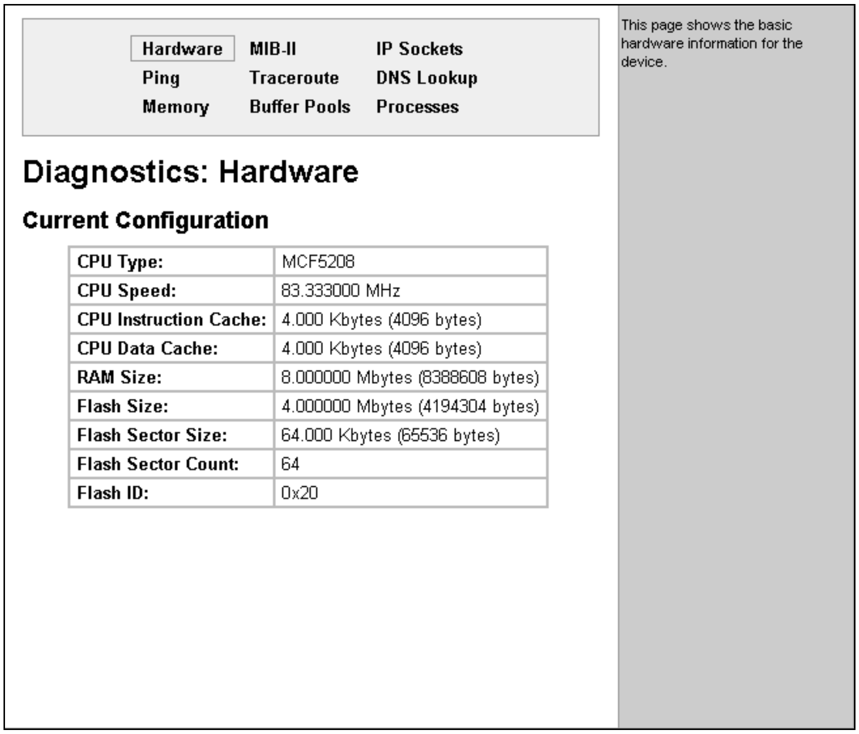
Hardware

This read-only page displays the current hardware configuration.

To display the MatchPort AR's hardware diagnostics:

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

Figure 4-45. Diagnostics: Hardware



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

This page shows the basic hardware information for the device.

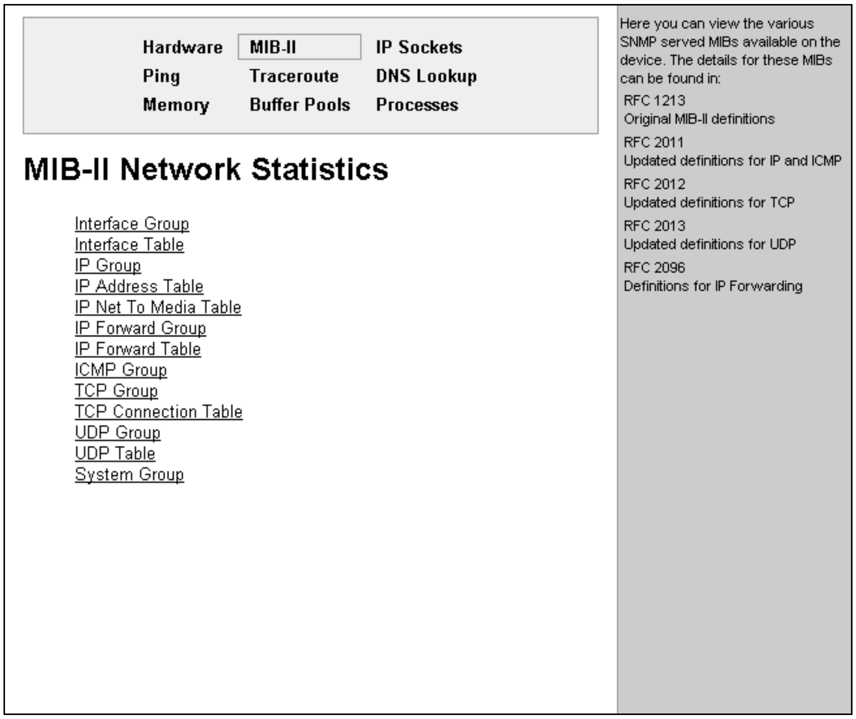
MIB-II Statistics

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

To view MatchPort AR’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 4-46. MIB-II Network Statistics



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

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

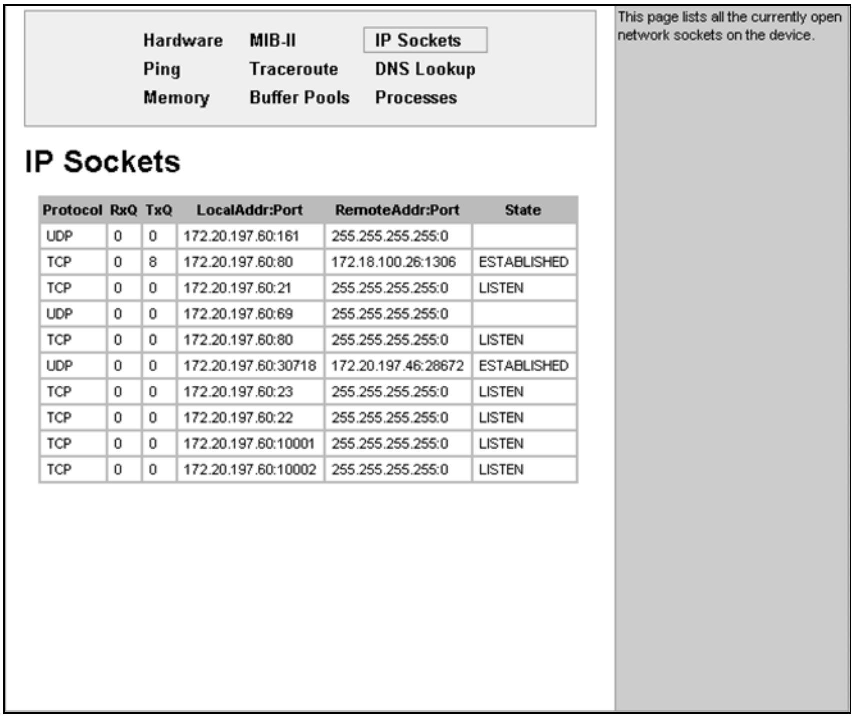
RFC 1213	Original MIB2 definitions.
RFC 2011	Updated definitions for IP and ICMP.
RFC 2012	Updated definitions for TCP.
RFC 2013	Updated definitions for UDP.
RFC 2096	Definitions for IP forwarding.

IP Sockets

To display open network sockets on the MatchPort AR:

1. 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 AR.

Figure 4-47. IP Sockets



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

IP Sockets

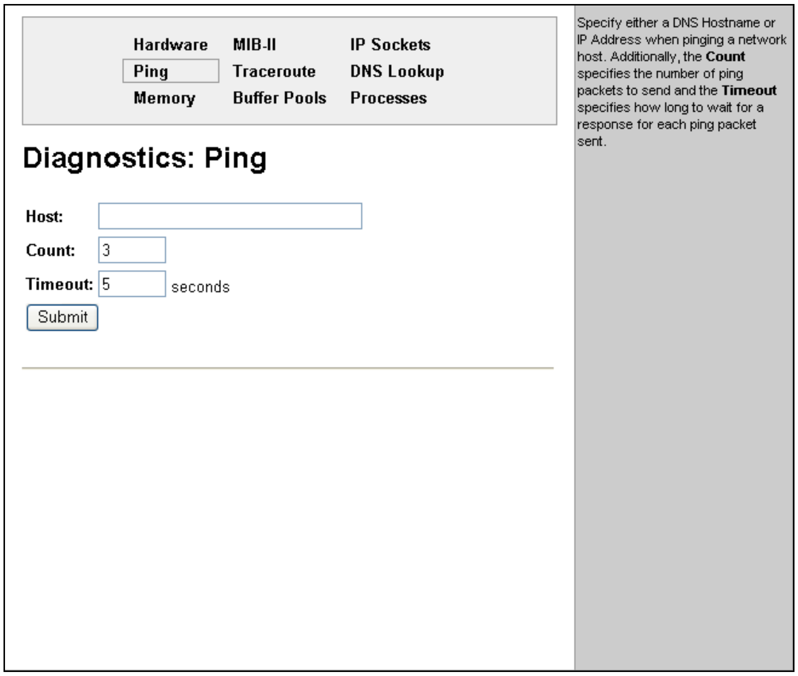
Protocol	RxQ	TxQ	LocalAddr:Port	RemoteAddr:Port	State
UDP	0	0	172.20.197.60:161	255.255.255.255:0	
TCP	0	8	172.20.197.60:80	172.18.100.26:1306	ESTABLISHED
TCP	0	0	172.20.197.60:21	255.255.255.255:0	LISTEN
UDP	0	0	172.20.197.60:69	255.255.255.255:0	
TCP	0	0	172.20.197.60:80	255.255.255.255:0	LISTEN
UDP	0	0	172.20.197.60:30718	172.20.197.46:28672	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

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 4-48. Diagnostics: Ping



Diagnostics: Ping

Host:

Count: 3

Timeout: 5 seconds

Specify either a DNS Hostname or IP Address when pinging a network host. Additionally, the **Count** specifies the number of ping packets to send and the **Timeout** specifies how long to wait for a response for each ping packet sent.

2. Enter or modify the following settings:

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

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

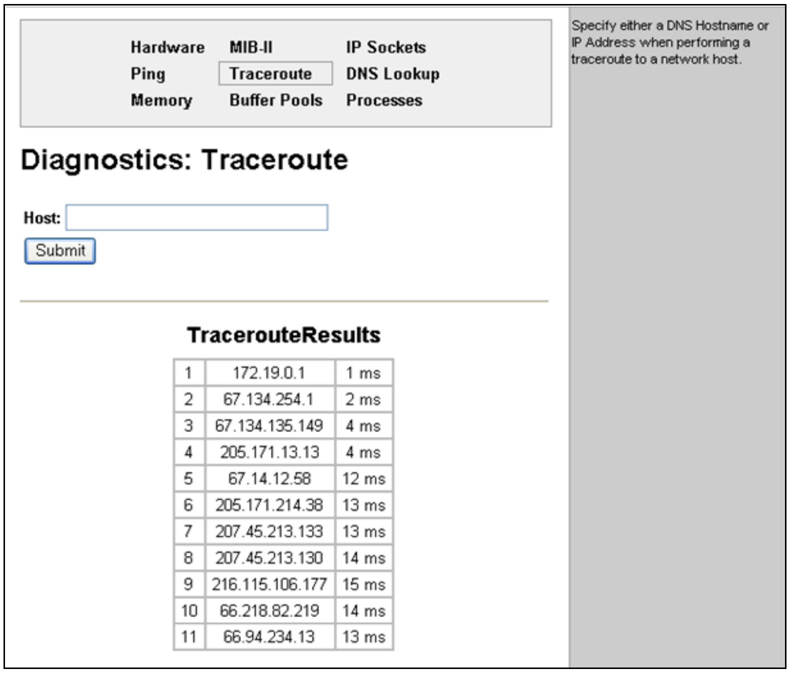
Traceroute

Here you can trace a packet from the MatchPort AR to an Internet host, showing how many hops the packet requires to reach the host and how long each hop takes. If you visit a web site whose pages appear slowly, you can use traceroute to determine where the longest delays are occurring.

To use traceroute from the MatchPort AR:

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

Figure 4-49. Diagnostics: Traceroute



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

Diagnostics: Traceroute

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 AR when issuing the traceroute command.

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

DNS Lookup

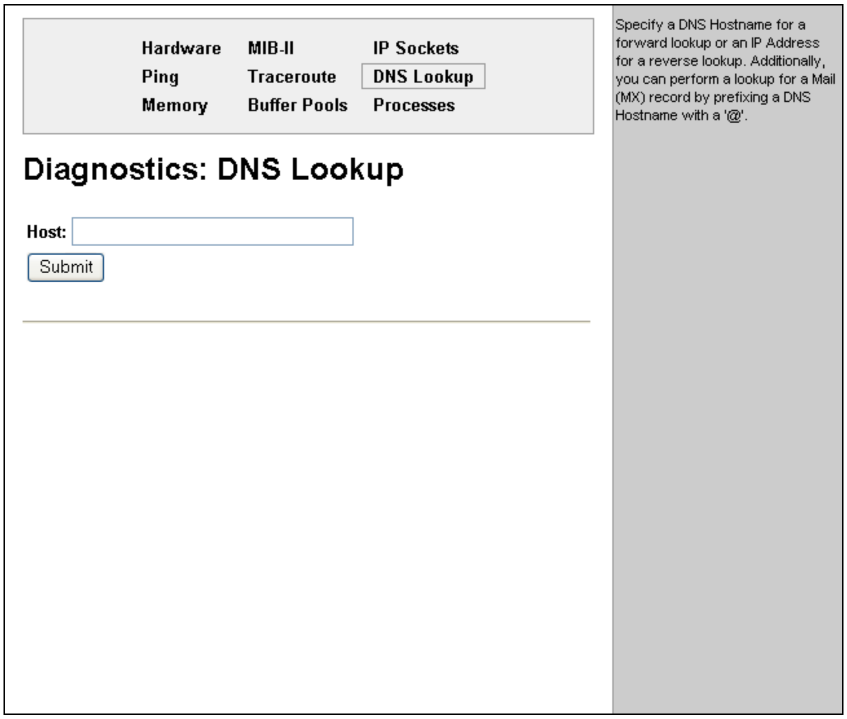
Here you can specify a DNS Hostname for a forward lookup or an IP address for a reverse lookup. You can also perform a lookup for a Mail (MX) record by prefixing a DNS Hostname with **@**.

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 4-50. Diagnostics: DNS Lookup



Specify a DNS Hostname for a forward lookup or an IP Address for a reverse lookup. Additionally, you can perform a lookup for a Mail (MX) record by prefixing a DNS Hostname with a '@'.

2. Enter or modify the following field:

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

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

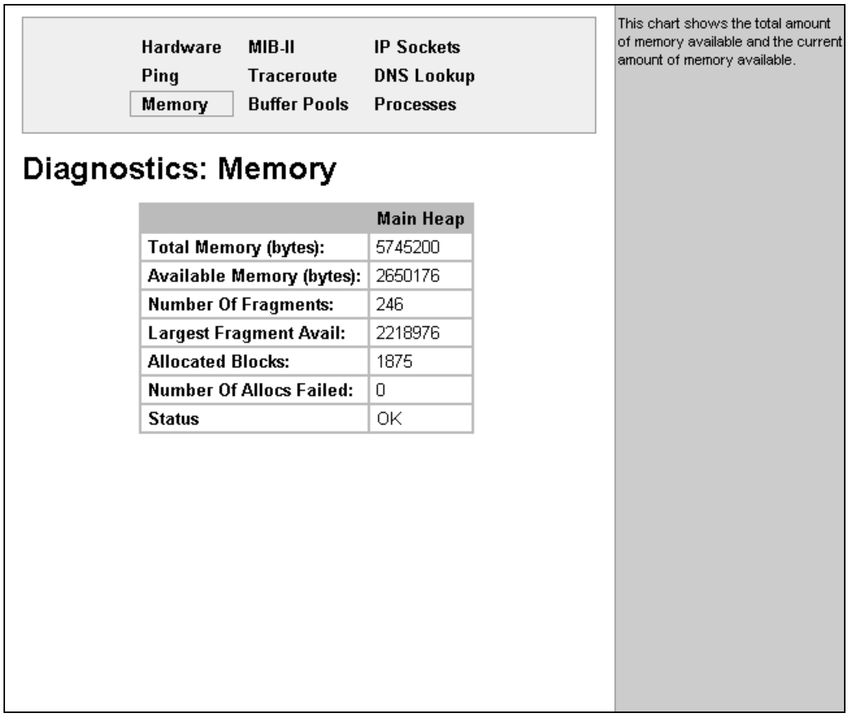
Memory

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 AR:

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

Figure 4-51. Diagnostics: Memory



Diagnostics: Memory

	Main Heap
Total Memory (bytes):	5745200
Available Memory (bytes):	2650176
Number Of Fragments:	246
Largest Fragment Avail:	2218976
Allocated Blocks:	1875
Number Of Allocs Failed:	0
Status	OK

This chart shows the total amount of memory available and the current amount of memory available.

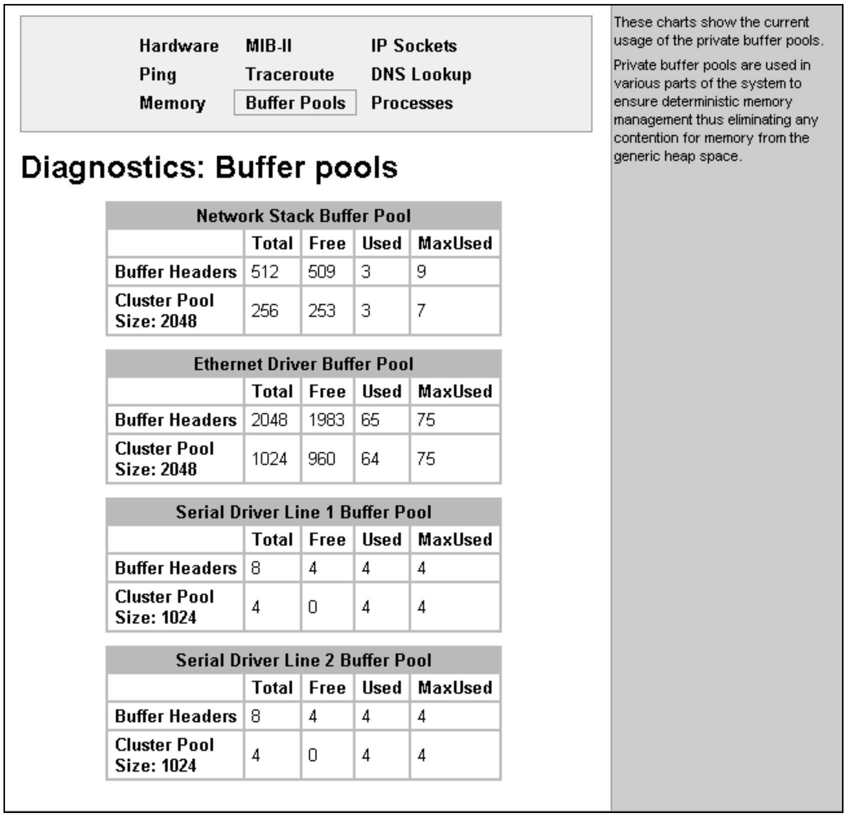
Buffer Pools

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

To display the MatchPort AR'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 4-52. Diagnostics: Buffer Pools



Diagnostics: Buffer pools

Network Stack Buffer Pool

	Total	Free	Used	MaxUsed
Buffer Headers	512	509	3	9
Cluster Pool Size: 2048	256	253	3	7

Ethernet Driver Buffer Pool

	Total	Free	Used	MaxUsed
Buffer Headers	2048	1983	65	75
Cluster Pool Size: 2048	1024	960	64	75

Serial Driver Line 1 Buffer Pool

	Total	Free	Used	MaxUsed
Buffer Headers	8	4	4	4
Cluster Pool Size: 1024	4	0	4	4

Serial Driver Line 2 Buffer Pool

	Total	Free	Used	MaxUsed
Buffer Headers	8	4	4	4
Cluster Pool Size: 1024	4	0	4	4

These charts show the current usage of the private buffer pools.

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

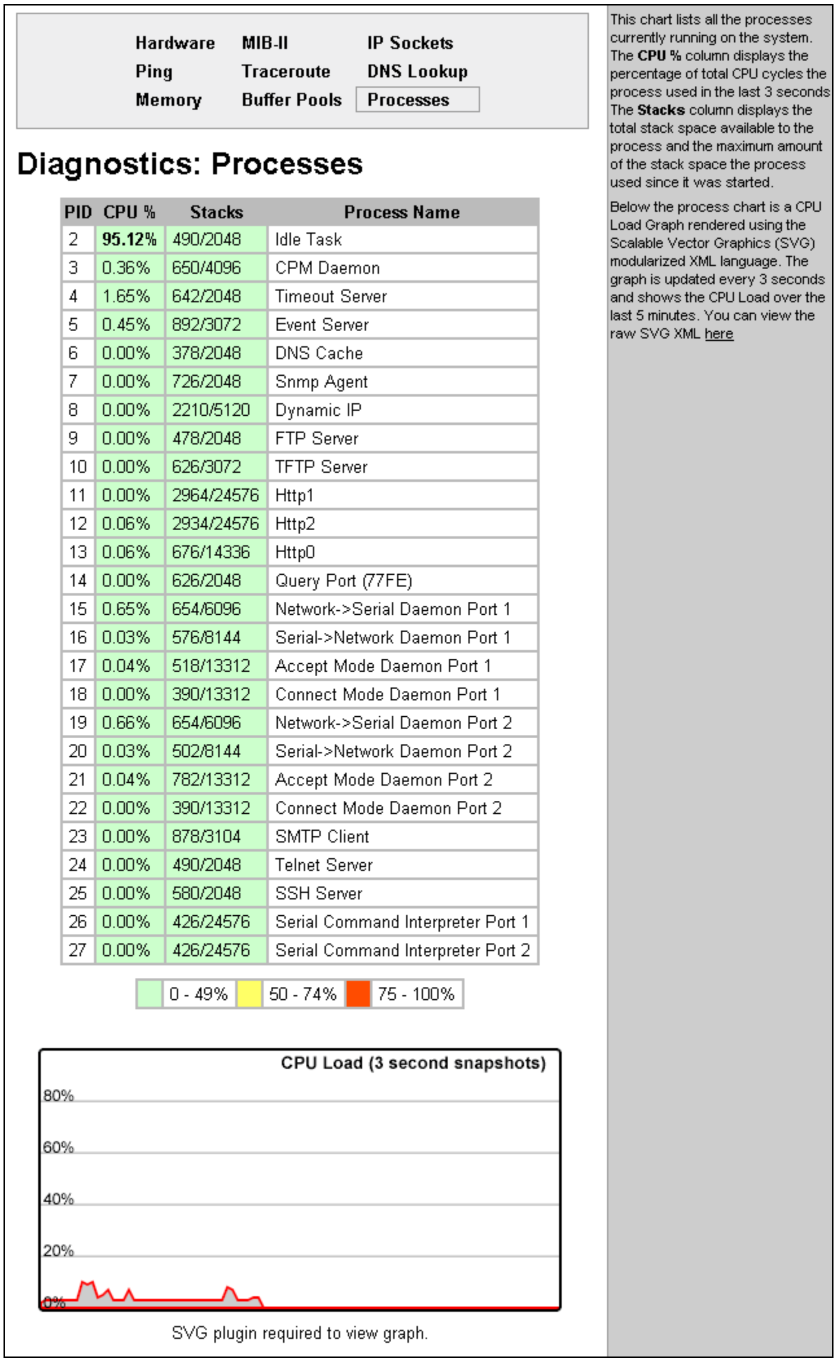
Processes

The MatchPort AR 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 AR 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 4-53. Diagnostics: Processes



Diagnostics: Processes

PID	CPU %	Stacks	Process Name
2	**95.12%**	490/2048	Idle Task
3	0.36%	650/4096	CPM Daemon
4	1.65%	642/2048	Timeout Server
5	0.45%	892/3072	Event Server
6	0.00%	378/2048	DNS Cache
7	0.00%	726/2048	Snmp Agent
8	0.00%	2210/5120	Dynamic IP
9	0.00%	478/2048	FTP Server
10	0.00%	626/3072	TFTP Server
11	0.00%	2964/24576	Http1
12	0.06%	2934/24576	Http2
13	0.06%	676/14336	Http0
14	0.00%	626/2048	Query Port (77FE)
15	0.65%	654/6096	Network->Serial Daemon Port 1
16	0.03%	576/8144	Serial->Network Daemon Port 1
17	0.04%	518/13312	Accept Mode Daemon Port 1
18	0.00%	390/13312	Connect Mode Daemon Port 1
19	0.66%	654/6096	Network->Serial Daemon Port 2
20	0.03%	502/8144	Serial->Network Daemon Port 2
21	0.04%	782/13312	Accept Mode Daemon Port 2
22	0.00%	390/13312	Connect Mode Daemon Port 2
23	0.00%	878/3104	SMTP Client
24	0.00%	490/2048	Telnet Server
25	0.00%	580/2048	SSH Server
26	0.00%	426/24576	Serial Command Interpreter Port 1
27	0.00%	426/24576	Serial Command Interpreter Port 2

🟩 0 - 49% 🟨 50 - 74% 🟥 75 - 100%

SVG plugin required to view graph.

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.

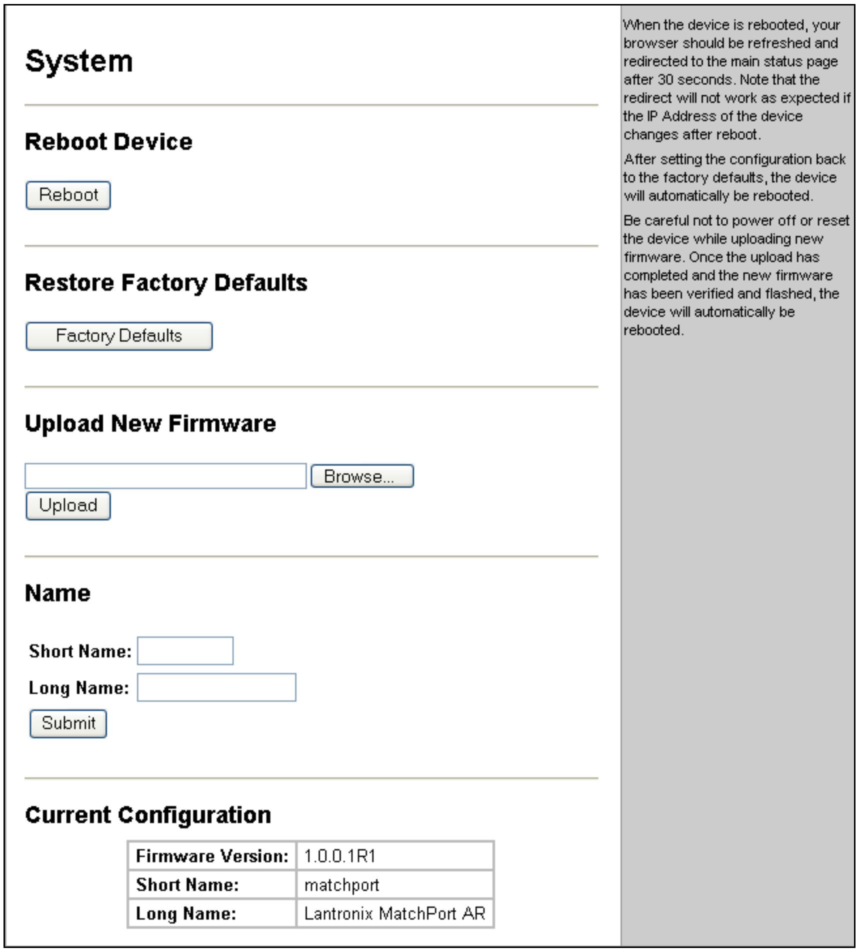
Below the process chart is a CPU Load Graph rendered using the Scalable Vector Graphics (SVG) modularized XML language. The graph is updated every 3 seconds and shows the CPU Load over the last 5 minutes. You can view the raw SVG XML here

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

System Configuration

The MatchPort AR 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 4-54. System



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 AR's system settings:

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

System Page Settings	Description
Reboot Device	Click **Reboot** to reboot the MatchPort AR. The system refreshes and redirects the browser to the MatchPort AR's home page.
Restore Factory Defaults	Click **Factory Defaults** to restore the MatchPort AR to the original factory settings. All configurations will be lost. The MatchPort AR automatically reboots upon setting back to the defaults.
Upload New Firmware	Click **Browse** to locate the firmware file location. Click **Upload**

System Page Settings	Description
	to install the firmware on the MatchPort AR. The device automatically reboots upon the installation of new firmware.
Name	Enter a new **Short Name** and a **Long Name** (if necessary). The **Short Name** maximum is 32 characters. The **Long Name** maximum is 64 characters. Changes take place upon the next reboot.

5: Point-to-Point Protocol (PPP)

***Note:** For instructions on configuring PPP for the MatchPort AR, see PPP on page 45.*

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 AR 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 AR'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 AR acts as the server side of the PPP link; it can require authentication and assign an IP address to the peer. Upon PPP configuration, IP packets are routed between Ethernet and PPP interfaces.

6: 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 27) or Command Mode's Tunnel Menu (see the MatchPort AR Command Reference for the full list of commands.)

The MatchPort AR 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 AR actively makes a connection. The receiving node on the network must listen for the Connect Mode's connection. Connect Mode is disabled by default.
- Accept Mode: the MatchPort AR listens for a connection. A node on the network initiates the connection. Accept Mode is enabled by default.
- Disconnect Mode: this mode defines how an open connection stops the forwarding of data. The specific parameters to stop the connection are configurable. Once the MatchPort AR'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 AR will not make a connection unless it can resolve the address. For DNS names, after 4 hours of an active connection, the MatchPort AR will re-evaluate the address. If it is a different address, it will close the connection.

Connect Mode supports the following protocols:

- TCP
- AES encryption over UDP
- AES encryption over TCP
- SSH (the MatchPort AR 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 AR 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 AR 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 AR, 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 AR is the SSH client. Ensure the MatchPort AR's SSH client username is configured on the remote SSH server before using it with the MatchPort AR.

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 AR 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 AR 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 AR 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 AR 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 AR 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 AR shuts down connections gracefully.

The following settings end a connection:

- The MatchPort AR receives the stop character.
- The timeout period has elapsed and no activity is going in or out of the MatchPort AR. Both Accept Mode and Connect Mode must be idle for the time frame.
- The MatchPort AR 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 AR packs the data and sends it out.
- The send character: Similar to a start or stop character, the MatchPort AR packs the data until it sees the send character. The MatchPort AR 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 AR 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 goes 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:

+++	Switches to Command Mode if entered from serial port during connection.
AT?	Help.
ATDT<Address Info>	Establishes the TCP connection to socket (<IP>/<port>).
ATDP<Address Info>	See ATDT.
ATD	Like ATDT. Dials default Connect Mode remote address and port.
ATD<Address Info>	Sets up a TCP connection. A value of 0 begins a command line interface session.
ATO	Switches to data mode if connection still exists. Vice versa to '+++'.
ATEn	Switches echo in Command Mode (off - 0, on - 1).
ATH	Disconnects the network session.
ATI	Displays modem information.
ATQn	Quiet mode (0 - enable results code, 1 - disable results code.)
ATVn	Verbose mode (0 - numeric result codes, 1 - text result codes.)
ATXn	Command does nothing and returns OK status.
ATUn	Accept unknown commands. (n value of 0 = off. n value of 1 = on.)

AT&V	Display current and saved settings.
AT&F	Reset settings in NVR to factory defaults.
AT&W	Save active settings to NVR.
ATZ	Restores the current state from the setup settings.
ATS0=n	Accept incoming connection. n value of 0 = disable n value of 1 = connect automatically n value of 2+ = connect with ATA command.
ATA	Answer incoming connection (if ATS0 is 2 or greater).
A/	Repeat last valid command.

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

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

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

When using ATDT and ATDP, enter 0.0.0.0 to switch to Command Mode. Once Command Mode is exited, the MatchPort AR reverts to modem emulation mode.

By default, the +++ characters are not passed through the connection. Turn on this capability using the **modem echo 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 AR 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 AR logs statistics for tunneling. The **Dropped** statistic displays connections ended by the remote location. The **Disconnected** statistic displays connections ended by the MatchPort AR.

7: SSH and SSL Security

The MatchPort AR supports Secure Shell (SSH) and Secure Sockets Layer (SSL). These security protocols are configurable through the Web Manager (see *SSH Settings* on page 60 and *SSL Settings* on page 67) and Command Mode (see the MatchPort AR Command Reference for available SSH and SSL commands).

Note: *This chapter overviews security configuration using Web Manager.*

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.

To configure the SSH settings, there are two instances that require configuration: when the MatchPort AR 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. Use the SSH client for tunneling in Connect Mode.

SSH Server Configuration

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

- Defined host keys: both private and public keys are required. They keys are used for the Diffie-Hellman key exchange (used for the underlying encryption protocol).
- Defined users: these users are permitted to connect to the MatchPort AR'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.

      i. SSH keys may be created on another computer and uploaded to the MatchPort AR. To do so, use the following command using Open SSH to create a 768-bit DSA key pair:

```
ssh-keygen -b 768 -t dsa
```

b) 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 AR 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 cryptography to offer authentication and privacy to message transmission over the Internet. Typically, only the server is authenticated. SSL allows the communication of client/server applications without eavesdropping and message tampering. SSL uses the public-and-private key encryption system from RSA, which also includes the use of a digital certificate.

SSL runs on layers between application protocols (HTTP, SMTP, etc.) and the TCP transport protocol. It is most commonly used with HTTP (thus forming HTTPS).

On the MatchPort AR, configure an SSL certificate for the HTTP server to listen on the HTTPS port. This certificate can be created elsewhere and uploaded to the device. Alternatively, it can be automatically generated on the device; this certificate type is a self-signed certificate.

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

To upload a new certificate or create a new self-signed certificate, see *SSL Settings* on page *67.*

8: Email

The MatchPort AR has a Simple Mail Transfer Protocol (SMTP) client. SMTP is a TCP/IP protocol used in sending and receiving email. Its objective is to send email efficiently and reliably.

There are three ways to send an email from the MatchPort AR:

1. Using the Web Manager (See *Configuration Using Web Manager* on page 18).
2. Using Command Mode by using the Send command (See the MatchPort AR Command Reference for available email commands under the Chem Menu).
3. By configuring a CP or a CP group (See *Configuration Pin Manager* on page 107). When the CP or the CP group changes state to the pre-specified value, an email alert is sent.

SMTP Configuration

This section covers email configuration using Command Mode. (For more information on Command Mode, see the MatchPort AR Command Reference.)

The minimum requirements for SMTP configuration are:

- At least one address configured for the “To” field or “Cc” field.
- The “From” address field configured.

Note: *A “Reply-To” field is also available for configuration. This differs from the “From” field in that all replies from the recipient will be sent to this address.*

When configuring the “To” and “Cc” settings, separate multiple addresses with a semi-colon (;).

The email queue separates email addresses by domain. One email is sent per domain (not per email address). The MatchPort AR makes a connection directly to the destination SMTP server instead of a relay server. This prevents the message from not reaching the recipient because of spam filters.

Use the **`File`** command for the body of the email’s text. The email’s text must be saved in a file; configure the location of this message file. The MatchPort AR permits entering a file path even if the file itself is not created yet. If the file does not exist when the email is sent, the body of the email reads “file does not exist”.

Priority Levels

The default priority level for the MatchPort AR's emails is Normal priority. The MatchPort AR has five configurable priority levels; certain recipient systems have filters based on these priority levels.

Configurable priority levels are:

Priority	**XPriority Level**
Urgent	1
High	2
Normal (default)	3
Low	4
Very Low	5

Some email programs may translate an Urgent priority to High, and Very Low priority to Low.

The MatchPort AR makes an SMTP connection to a destination server. By default, it connects to the destination's port 25. Override this port number by using the **`Server Port`** command.

DNS Records

Domain Name Service (DNS) translates text-based domain names to the numeric IP addresses necessary for locating the domain's server on the Internet. Many DNS servers have multiple records per domain. To resolve these addresses, the MatchPort AR's DNS server listing looks for MX records first. MX is the Mail Exchange Record; it is an entry in the domain name table identifying the mail server responsible for managing emails for that domain name.

If the MX record is not available, then the DNS server uses the default record. If it cannot find the default record, it will not send the email.

Extended Hello

When the MatchPort AR makes a connection to the recipient's SMTP server, it sends an EHLO message. This message contains the MatchPort AR's domain.

Use the **`Overriding Domain`** command to change the domain provided in the EHLO message.

For more information on EHLO, see RFC 2821.

Email Statistics

Use the **`Show Statistics`** command to display the MatchPort AR's email statistics.

Use the `Show Log` command to display the email log. When the system sends an email, the following information is logged:

1. Messages the MatchPort AR sends to the SMTP server.
2. Messages from the SMTP server to the MatchPort AR.
3. SMTP commands and replies.

Note: *The MatchPort AR does not log email message contents.*

9: Configuration Pin Manager

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

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 AR into another system.

Each CP group is a 32 bit variable. When a CP is added to a CP group, it is assigned to a bit position within the group. A CP cannot be assigned to a group until it is configured. A CP can be a member of multiple groups, but may only be active in one.

There are a fixed number of pre-defined CP groups that enable standard functions such as Modem Control (DTR and DCD) and RS485 chip selection. You can assign any CP to these pre-defined groups. The following table lists the pre-defined groups available on the MatchPort AR:

CP Group	Function
Line1_Select_RS485	Control RS232/RS485 mode toggle for external transceiver on Serial Port 1
Line1_Hlf_Dplx_RS485	Control RS485 half-duplex/full duplex mode toggle for external transceiver on Serial Port 1
Line1_Modem_Cntl_Out	Control Line for DSR/DTR mode on Serial Port 1
Line1_Modem_Cntl_In	Control Line for DSR/DTR mode on Serial Port 1
Line2_Modem_Cntl_Out	Control Line for DSR/DTR mode on Serial Port 2
Line2_Modem_Cntl_In	Control Line for DSR/DTR mode on Serial Port 2

The Configurable Pin Manager (CPM) is available through the Web Manager (see *Configuration Using Web Manager* on page 18) or through Command Mode (see the MatchPort AR Command Reference for available commands in the CPM Menu).

Configurable Pins

To view a CP's configuration:

1. If using the Web Manager:

   a) Click **CPM → CPs** at the top of the page. The CPM: Configurable Pin page displays.

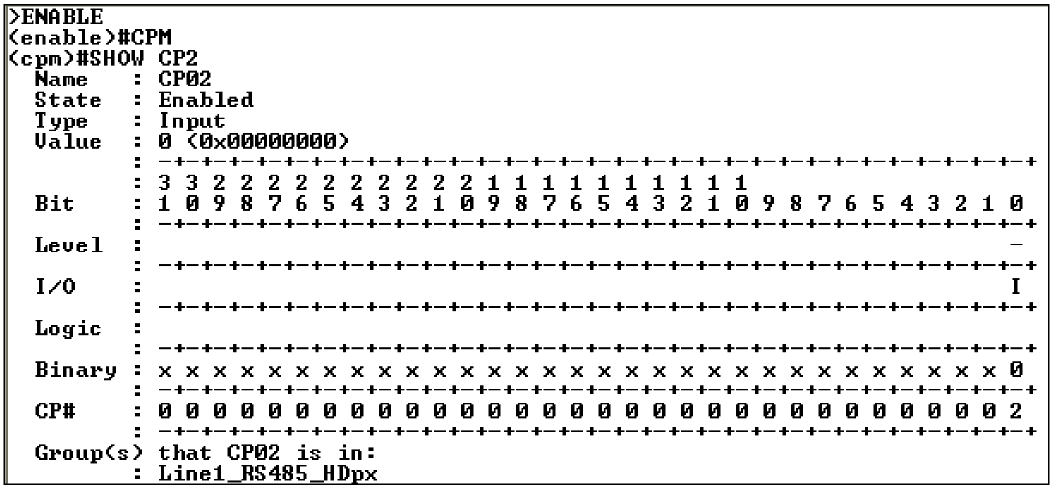
   b) Click the specific **CP** from the Current Configuration table. The CP's configuration displays in the CP Status table.

2. If using Command Mode (the CLI):

   a) Enter **`Enable`** → **`CPM`** to access the CPM level menu.

b) Type **`show cp`**. The CP table displays:

Figure 9-1. CP Table on the CLI



```
>ENABLE
(enable)#CPM
(cpm)#SHOW CP2
  Name     : CP02
  State    : Enabled
  Type     : Input
  Value    : 0 (0x00000000)
           : -+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
           : 3 3 2 2 2 2 2 2 2 2 2 2 1 1 1 1 1 1 1 1 1 1
  Bit      : 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
           : -+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
  Level    :                                                               -
           : -+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
  I/O      :                                                               I
           : -+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
  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 0
           : -+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
  CP#      : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 2
           : -+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
  Group(s) that CP02 is in:
           : Line1_RS485_HDpx
```

3. View the following:

CPs: Current Configuration	Description
Name	Name of the configurable pin.
State	Indicates whether the pin is enabled or disabled.
Type	Indicates whether the pin is set for input or output.
Value	The CP's current value (**0** or **1**).
Bit	Visual display of the 32-bit placeholders for a CP group.
Level	Shows voltage as high (**+**) or low (**-**).
I/O	Indicates the current status of the pin: **I** = input **0** = output **X** = unassigned
Logic	**I** = CP is inverted (so that assertion is low)
Binary	Shows the current value of the bit.
CP#	Indicates the CP number.
Groups	Indicates the groups in which the CP is a member.

CP Groups

To view a CP group's configuration:

1. If using the Web Manager:

   a) Click **CPM → Groups** at the top of the page. The CPM: Groups page displays.

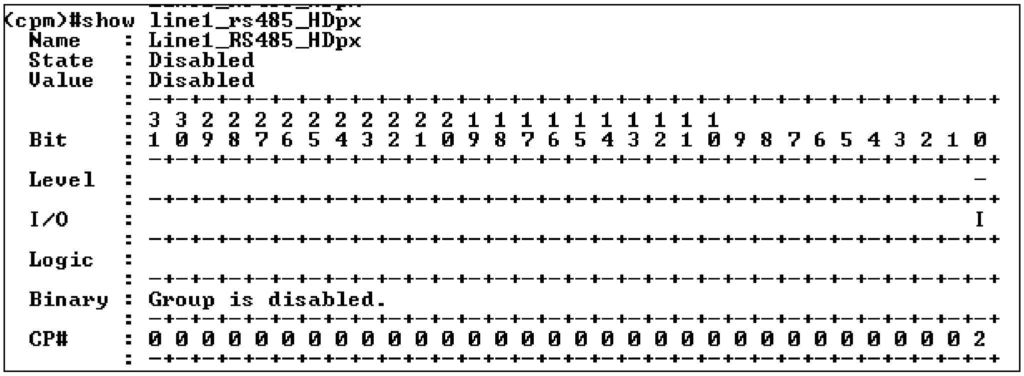
   b) Click the CP groups from the Current Configuration table. The CP's configuration displays in the Group Status table.

2. If using Command Mode (the CLI):

   a) Enter **`Enable`** → **`CPM`** to access the CPM level menu.

   b) Type **`show <name>`**.The Group Status table displays the following:

Figure 9-2. CP Group Table on the CLI



```
(cpm)#show line1_rs485_HDpx
  Name   : Line1_RS485_HDpx
  State  : Disabled
  Value  : Disabled
         : -+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
         : 3 3 2 2 2 2 2 2 2 2 2 2 1 1 1 1 1 1 1 1 1 1
  Bit    : 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
         : -+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
  Level  :                                                               -
         : -+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
  I/O    :                                                               I
         : -+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
  Logic  :
         : -+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
  Binary : Group is disabled.
         : -+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
  CP#    : 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 2
         : -+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

2. View the following:

Name	Name of the selected group.
State	Indicates whether the group is enabled, disabled, or locked.
Value	Displays the last bit in the CP's current value.
Bit	Visual display of the 32-bit placeholders for a CP group.
Level	Shows voltage as high (**+**) or low (**-**).
I/O	A "+" symbol indicates the CP is asserted (the voltage is high). A "-"indicates the CP voltage is low.
Logic	An "**I**" indicates the CP is inverted (so that the assertion is low).
Binary	Displays the assertion value of the bit.
CP#	Displays the CP number.

The CP group table displays the CPs assigned to it. It also displays the CP's bit position within the CP group.

To configure a group's value:

1. If using the Web Manager:

   a) Click **CPM → Groups** at the top of the page. The CPM Groups page displays

   b) To create a CP group:

      i. Enter a group name in the **Create Group** field.

      ii. Click **Submit**. Changes are applied immediately to the MatchPort AR.

   c) To delete a CP group:

      i. Select the CP group from the **Delete Group** drop-down list.

      ii. Click **Submit**. Changes are applied immediately to the MatchPort AR.

   d) To enable or disable a CP group:

      i. Select the CP group from the **Set** drop-down list.

      ii. Select the state (**Enabled** or **Disabled**) from the drop-down list.

      iii. Click **Submit**. Changes are applied immediately to the MatchPort AR.

   e) To set a CP group's value:

      i. Select the CP group from the **Set** drop-down list.

      ii. Enter the CP group's value in the **value** field.

      iii. Click **Submit**. Changes are applied immediately to the MatchPort AR.

   f) To add a CP to a CP group:

      i. Select the CP from the **Add** drop-down list.

      ii. Select the CP group from the drop-down list.

      iii. Select the CP's bit location from the **bit** drop-down menu.

      iv. Click **Submit**. Changes are applied immediately to the MatchPort AR.

   g) To delete a CP from a CP group:

      i. Select the CP from the **Remove** drop-down list.

      ii. Select the CP group from the drop-down list.

      iii. Click **Submit**. Changes are applied immediately to the MatchPort AR.

2. If using Command Mode:

   a) Enter **`enable`** → **`cpm`** to access the CPM level menu.

   b) Use the add, delete, and set commands to configure values within Command Mode (for more information on these parameters, see the MatchPort AR Command Reference).

Note: *Each CP with a bit position value of 1 (when the decimal value is converted to binary) has an asserted state.*

10: XML

The MatchPort AR provides an Extensible Markup Language (XML) interface that can be used to configure MatchPort AR devices. Every configuration setting that can be issued from the MatchPort AR Web Manager and CLI can also be specified using XML.

The MatchPort AR can import and export configuration settings as an XML document known as an XML configuration record (XCR). An XCR can be imported or exported via the CLI, a Web browser, FTP, or the MatchPort AR's filesystem. An XCR being imported or exported can contain many configuration settings or just a few. For example, it might change all of the configurable parameters for a MatchPort AR, or it may only change the baud rate for a single serial line. Using XCRs provides a straightforward and flexible way to manage the configuration of multiple MatchPort AR devices.

For more information on using XML for MatchPort AR configuration, see the MatchPort AR Command Reference.

11: Branding the MatchPort AR

The MatchPort AR'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. For more on the filesystem, see Filesystem Configuration on page 75.*

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

Command Mode

Customize the MatchPort AR'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 AR
```

To change the MatchPort AR's short and long names:

1. Click **System** at the top of the page. The System page opens.

1. In the **Short Name** field, enter the new short name for the device (up to 32 characters).

2. In the **Long Name** field, enter the new long name for the device (up o 64 characters).

3. Click **Submit**.

4. To apply changes, click **Reboot**.

12: 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 AR'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 AR. 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 or eu_support@lantronix.com

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

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

- Your name, and your company name, address, and phone number
- Lantronix model number
- Lantronix serial number
- 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 hexadecimals or to look up hexadecimal values in the tables of configuration options. The tables include:

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

Converting Binary to Hexadecimal

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

Conversion Table

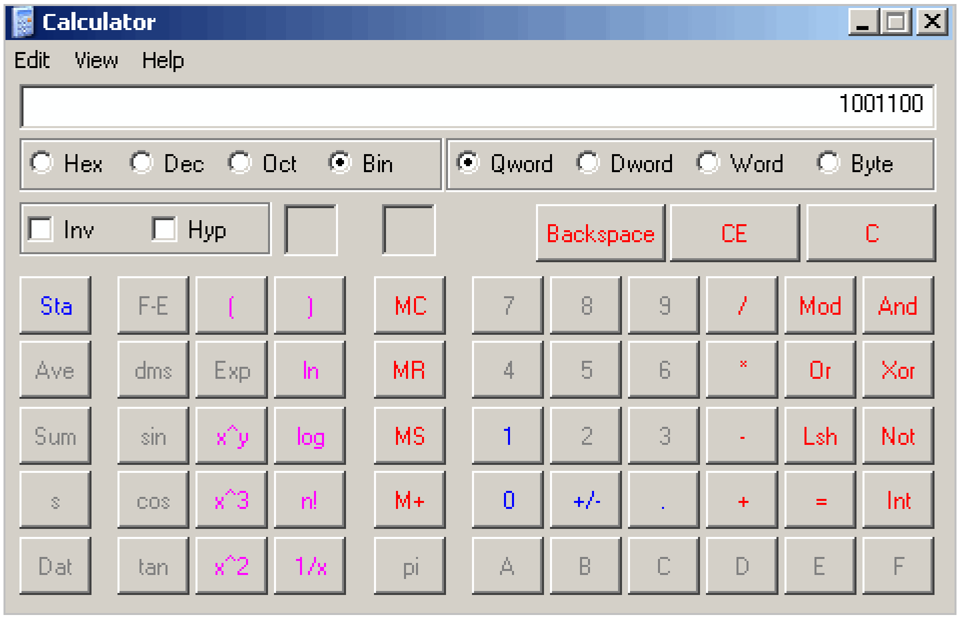
Hexadecimal digits have values ranging from 0 to F, which are represented as 0-9, A (for 10), B (for 11), etc. To convert a binary value (for example, 0100 1100) to a hexadecimal representation, treat the upper and lower four bits separately to produce a two-digit hexadecimal number (in this case, 4C).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


Calculator
Edit View Help
Backspace CE C
Sta F-E ( ) MC 7 8 9 / Mod And
Ave dms Exp ln MR 4 5 6 * Or Xor
Sum sin x^y log MS 1 2 3 - Lsh Not
s cos x^3 n! M+ 0 +/- . + = Int
Dat tan x^2 1/x pi A B C D E F

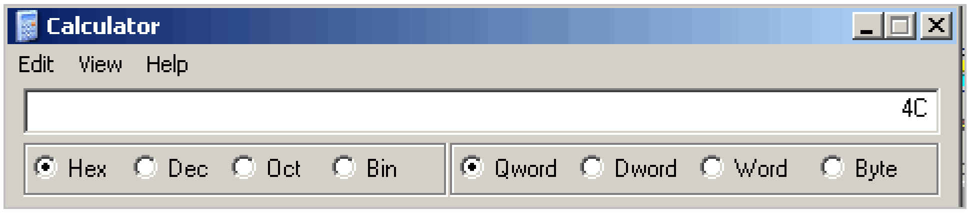
1001100

○ Hex ○ Dec ○ Oct ● Bin

● Qword ○ Dword ○ Word ○ Byte

□ Inv □ Hyp

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



4C

● Hex ○ Dec ○ Oct ○ Bin

● Qword ○ Dword ○ Word ○ Byte

C: Warranty

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

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

* * * *

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

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

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

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

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