XPort AR User Guide

Part Number 900-405
Revision G December 2010

Copyright & Trademark

Warranty

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

Contacts

Lantronix Corporate Headquarters

167 Technology Drive
Irvine, CA 92618, USA
Phone:949-453-3990
Fax:949-450-7249

Technical Support

Online: www.lantronix.com/support

Sales Offices

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

Disclaimer

Note: *This product has been designed to comply with the limits for a Class A digital device pursuant to 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. See "Appendix - Compliance" on page 131 for additional information.*

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

Revision History

Date	Rev.	Comments
June 2005	A	Initial Document
November 2005	B	Added V2.0 software information.
December 2006	C	Added V3.0 software information.
March 2007	D	Corrected pin numbers.
June 2009	E	Updated to firmware V4.0.0.0R16.
May 2010	F	Updated to firmware V5.1.0.0R10.
December 2010	G	Updated for firmware version 5.2.0.0R21. Added improvements to SNMP, logging and SSL.

Table of Contents

List of Figures

List of Tables

1: About This Guide

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

Chapter and Appendix Summaries

A summary of each chapter is provided below.

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

Additional Documentation

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

Document	Description
XPort AR Integration Guide	Information about the XPort AR hardware and evaluation board along with directions on integrating XPort AR into your product.
XPort AR Command Reference	Instructions for accessing the Command Mode (the command line interface) using a Telnet connection or th rough the serial port. Detailed information about the comands. Alos provides details for XML configuration and status.
XPort AR Getting Started Guide	Instructions for getting the XPort AR on the evaluation board up and running.
DeviceInstaller Online Help	Instructions for using the Lantronix Windows-based utility to locate the device 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

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

This chapter contains the following sections:

Key Features

Note: *Consult the Integration Guide for more detailed hardware information.*

- Power Supply: Regulated 3.3V input required.
- Controller: A Lantronix DSTni-EX CPU with 256 kB zero wait state SRAM and 16 Kbytes of boot ROM.
- Memory: 4 MB Flash and 1.25 MB SDRAM.
- Ethernet: 10/100 Mbps Ethernet transceiver
- Serial Ports: Two full serial ports with all hardware handshaking signals or three serial ports without handshaking signals. Baud rate is software selectable (300 bps to 230400 bps).
- Fully compliant PoE designs by using PoE compliant magnetics and passing through both the used and unused pairs.
- Configurable IO Pins (CPs): Up to eleven pins are configurable as general purpose I/Os if no modem control signal is used on serial ports. All I/O pins are 5V tolerant.
- Interface Signals: 3.3V-level interface signals.
- Temperature Range: Operates over an extended temperature range of -40°C to +85°C.

Applications

The XPort 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 unit
- Telecommunications equipment
- Handheld instruments
- Data display devices
- Security alarms and access control devices
- Modems
- Time/attendance clocks and terminalsPatient monitoring equipment
- Medical instrumentation
- Industrial Manufacturing/Automation systems
- Building Automation equipment
- Point of Sale Systems

Protocol Support

The XPort AR device server contains a full-featured TCP/IP stack. Supported protocols include:

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

Evolution OS™

The XPort AR incorporates The Lantronix Evolution OS™. Key features of the Evolution OS™ include:

- Built-in Web server for configuration and troubleshooting from Web-based browsers
- CLI configurability
- SNMP management
- XML data transport and configurability
- Really Simple Syndication (RSS) information feeds
- Enterprise-grade security with SSL and SSH
- Comprehensive troubleshooting tools

Additional Features

Modem Emulation

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

Web-Based Configuration and Troubleshooting

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

Command-Line Interface (CLI)

Making the edge-to-enterprise vision a reality, the XPort 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 XPort 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 XPort AR.

XML-Based Architecture and Device Control

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

Really Simple Syndication (RSS)

The XPort AR supports Really Simple Syndication (RSS) for streaming and managing on-line content. RSS feeds all the configuration changes that occur on the device. An RSS aggregator then reads (polls) the feed. More powerful than simple email alerts, RSS uses XML as an underlying Web page transport and adds intelligence to the networked device, while not taxing already overloaded email systems.

Enterprise-Grade Security

Evolution OS™ provides the XPort AR the highest level of networking security possible. This ‘data center grade’ protection ensures that each device on the M2M network carries the same level of security as traditional IT networking equipment in the corporate data center.

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

SSH and SSL are able to do the following:

- Verify the data received came from the proper source

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

In addition to keeping data safe and accessible, the XPort 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 XPort AR cannot be used to bring down other devices on the network.

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

Terminal Server/Device Management

Remote offices can have routers, PBXs, servers and other networking equipment that require remote management from the corporate facility. The XPort AR easily attaches to the serial ports on a server, Private Branch Exchange (PBX), or other networking equipment to deliver central, remote monitoring and management capability.

Troubleshooting Capabilities

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

Configuration Methods

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

DeviceInstaller: Configure the IP address and related settings and view current settings on the using a Graphical User Interface (GUI) on a PC attached to a network. See *Using DeviceInstaller (on page 19)*.

Web Manager: Through a web browser, configure the XPort AR settings using the Lantronix Web Manager. See *Configuration Using Web Manager (on page 21)*.

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

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

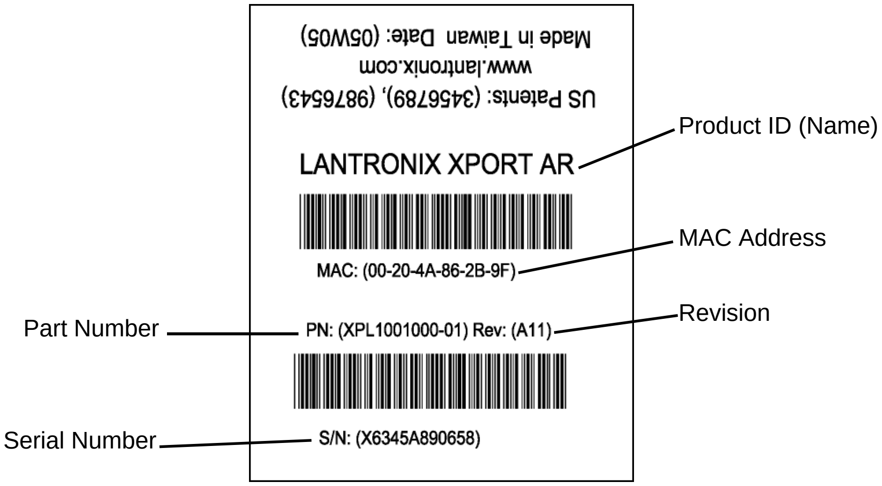
Product Information Label

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

- Bar Code
- Product ID (name)

- Product Revision
- Part Number
- Hardware Address (MAC Address or Serial Number)

Figure 2-2 Product Label



3: Using DeviceInstaller

This chapter covers the steps for locating a device and viewing its properties and details. DeviceInstaller is a free utility program provided by Lantronix that discovers, configures, upgrades and manages Lantronix Device Servers. It can be downloaded from the Lantronix website at www.lantronix.com/support/downloads.html. For instructions on using DeviceInstaller to configure the IP addres, related settings or for more advanced features, see the DeviceInstaller online help.

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

Accessing XPort AR Using DeviceInstaller

Note: Make note of the MAC address. It is needed to locate the XPort AR using DeviceInstaller.

1. Click **Start > All Programs > Lantronix > DeviceInstaller > DeviceInstaller.**

   When DeviceInstaller starts, it will perform a network device search. To perform another search, click the “Search” button.

2. Expand the XPort AR folder by clicking the **+** symbol next to the XPort AR folder icon. The list of available Lantronix XPort AR devices appears.
3. Select the XPort AR unit by expanding its entry and clicking on its hardware (MAC) address to view its configuration.
4. On the right page, click the **Device Details** tab. The current XPort AR configuration appears. This is only a subset of the full configuration; the complete configuration may be accessed via Web Manager, CLI, or XML.

Device Details Summary

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

Current Settings	Description
Name	Name identifying the XPort AR.
DHCP Device Name	Shows the name associated with the XPort AR’s current IP address, if the IP address was obtained dynamically.
Group	Configurable field. Enter a group to categorize the XPort AR. Double-click the field, type in the value, and press Enter to complete. This group name is local to this PC and is not visible on other PCs or laptops using DeviceInstaller.
Comments	Configurable field. Enter comments for the XPort 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	Shows the XPort AR device family type as “XPort”.
Type	Shows the device type as “XPort AR”.

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

4: Configuration Using Web Manager

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

Accessing Web Manager

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

To access Web Manager, perform the following steps:

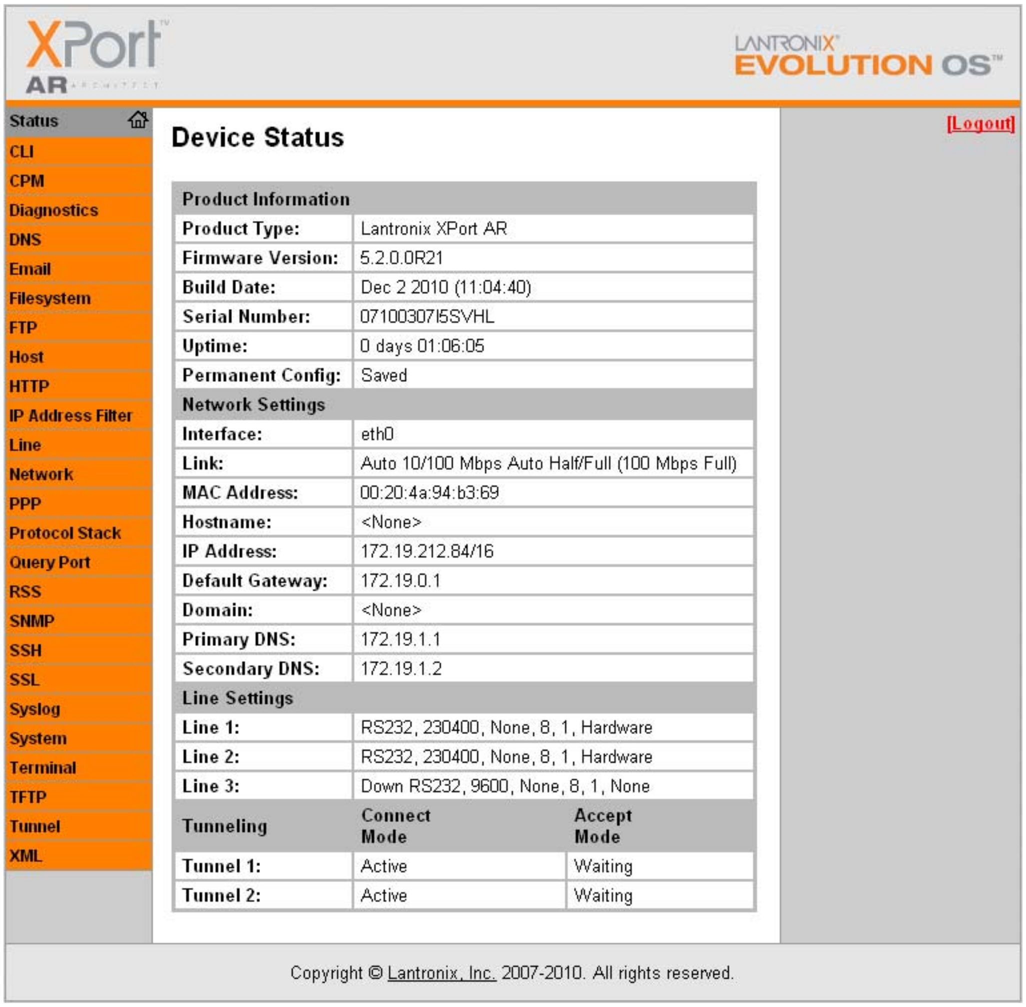
1. Open a standard web browser. Lantronix supports the latest version of Internet Explorer, Mozilla Suite, Mozilla Firefox, Safari, Chrome or Opera.
2. Enter the IP address of the XPort AR in the address bar. The IP address may have been assigned manually using DeviceInstaller (see the *XPort AR Quick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

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

Device Status Page

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

Figure 4-1 Web Manager Home Page



Device Status

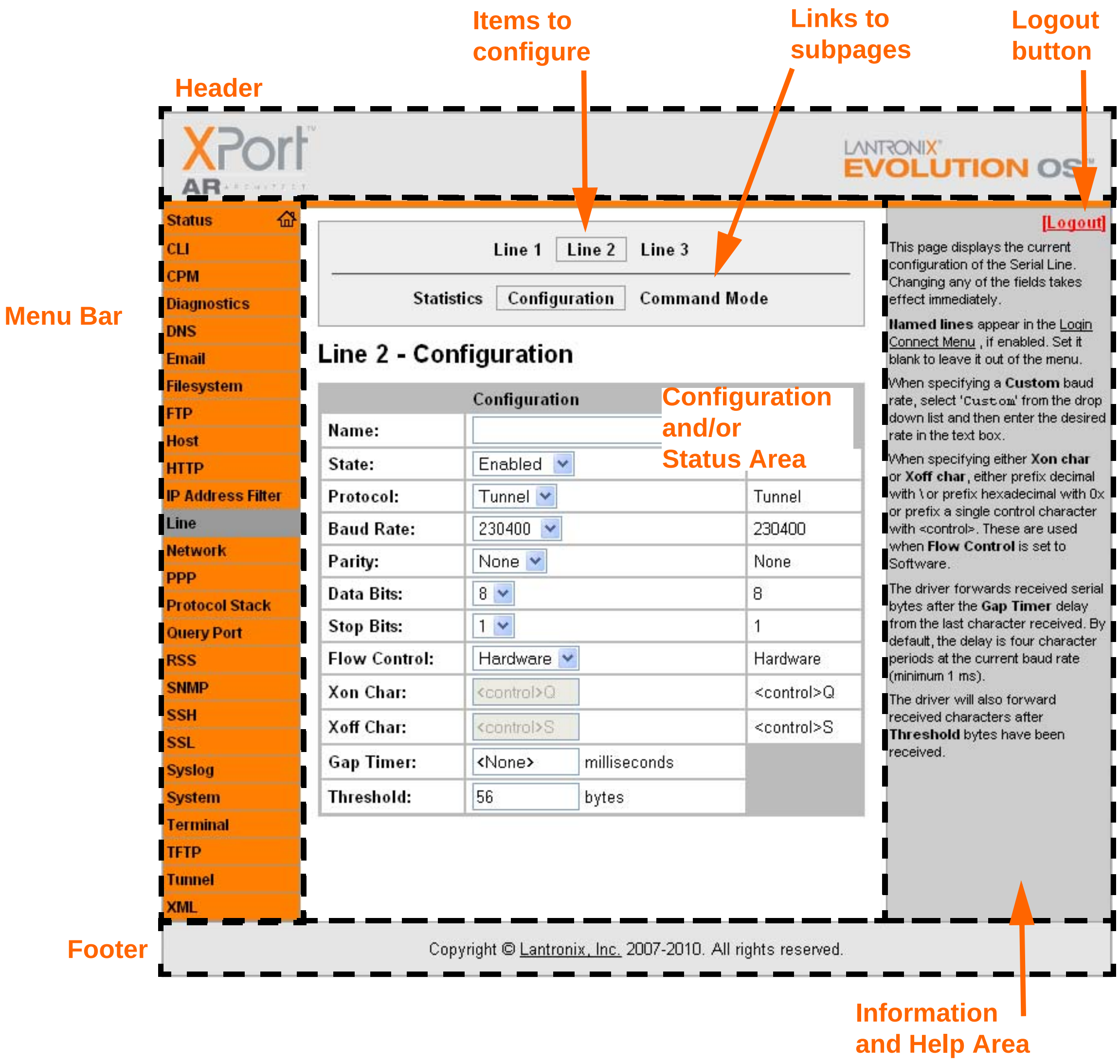
Product Information		
Product Type:	Lantronix XPort AR	
Firmware Version:	5.2.0.0R21	
Build Date:	Dec 2 2010 (11:04:40)	
Serial Number:	07100307I5SVHL	
Uptime:	0 days 01:06:05	
Permanent Config:	Saved	
Network Settings		
Interface:	eth0	
Link:	Auto 10/100 Mbps Auto Half/Full (100 Mbps Full)	
MAC Address:	00:20:4a:94:b3:69	
Hostname:	<None>	
IP Address:	172.19.212.84/16	
Default Gateway:	172.19.0.1	
Domain:	<None>	
Primary DNS:	172.19.1.1	
Secondary DNS:	172.19.1.2	
Line Settings		
Line 1:	RS232, 230400, None, 8, 1, Hardware	
Line 2:	RS232, 230400, None, 8, 1, Hardware	
Line 3:	Down RS232, 9600, None, 8, 1, None	
Tunneling	**Connect Mode**	**Accept Mode**
Tunnel 1:	Active	Waiting
Tunnel 2:	Active	Waiting

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

Web Manager Page Components

The layout of a typical Web Manager page is below.

Figure 4-2 Components of the Web Manager Page



Line 2 - Configuration

Configuration		
Name:		
State:	Enabled	
Protocol:	Tunnel	Tunnel
Baud Rate:	230400	230400
Parity:	None	None
Data Bits:	8	8
Stop Bits:	1	1
Flow Control:	Hardware	Hardware
Xon Char:	<control>Q	<control>Q
Xoff Char:	<control>S	<control>S
Gap Timer:	<None> milliseconds	
Threshold:	56 bytes	

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

Named lines appear in the Login Connect Menu , if enabled. Set it blank to leave it out of the menu.

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 prefix a single control character with <control>. These are used when **Flow Control** is set to Software.

The driver forwards received serial bytes after the **Gap Timer** delay from the last character received. By default, the delay is four character periods at the current baud rate (minimum 1 ms).

The driver will also forward received characters after **Threshold** bytes have been received.

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

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

The main area of the page has these additional sections:

- At the very top, many pages, such as the one in the example above, enable you to link to sub pages. On some pages, you must also select the item you are configuring, such as a line or a tunnel.
- In the middle of many pages, you can select or enter new configuration settings. Some pages show status or statistics in this area rather than allow you to enter settings.

- At the bottom of most pages, the current configuration is displayed. In some cases, you can reset or clear a setting.
- The information or help area shows information or instructions associated with the page.
- A **Logout** link is available at the upper right corner of every web page. In Chrome or Safari, it is necessary to close out of the browser to logout. If necessary, reopen the browser to log back in.
- The footer appears at the very bottom of the page. It contains copyright information and a link to the Lantronix home page.

Navigating the Web Manager

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

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

Table 4-3 **Summary of Web Manager Pages**

Web Manager Page	Description	See Page
Status	Shows product information and network, line, and tunneling settings.	*30*
CLI	Shows Command Line Interface (CLI) statistics and lets you change the current CLI configuration settings.	*114*
CPM	Shows information about the Configurable Pins Manager (CPM) and how to set the configurable pins and pin groups to work with a device.	*54*
Diagnostics	Lets you perform various diagnostic procedures.	*99*
DNS	Shows the current configuration of the DNS subsystem and the DNS cache.	*62*
Email	Shows email statistics and lets you clear the email log, configure email settings, and send an email.	*111*
Filesystem	Shows file system statistics and lets you browse the file system to view a file, create a file or directory, upload files using HTTP, copy a file, move a file, or perform TFTP actions.	*88*
FTP	Shows statistics and lets you change the current configuration for the File Transfer Protocol (FTP) server.	*66*
Host	Lets you view and change settings for a host on the network.	*53*
HTTP	Shows HyperText Transfer Protocol (HTTP) statistics and lets you change the current configuration and authentication settings.	*68*
IP Address Filter	Lets you specify all the IP addresses and subnets that are allowed to send data to this device.	*97*
Line	Shows statistics and lets you change the current configuration and Command mode settings of a serial line.	*30*

Web Manager Page (continued)	Description	See Page
Network	Shows status and lets you configure the network interface.	*26*
PPP	Lets you configure a network link using Point-to-Point Protocol (PPP) over a serial line.	*63*
Protocol Stack	Lets you perform lower level network stack-specific activities.	*92*
Query Port	Lets you change configuration settings for the query port.	*98*
RSS	Lets you change current Really Simple Syndication (RSS) settings.	*73*
SNMP	Lets you change the current Simple Network Management Protocol (SNMP) configuration settings.	*64*
SSH	Lets you change the configuration settings for SSH server host keys, SSH server authorized users, SSH client known hosts, and SSH client users.	*75*
SSL	Lets you upload an existing certificate or create a new self-signed certificate.	*82*
Syslog	Lets you specify the severity of events to log and the server and ports to which the syslog should be sent.	*67*
System	Lets you reboot device, restore factory defaults, upload new firmware, and change the device long and short names.	*109*
Terminal	Lets you change current settings for a terminal.	*50*
TFTP	Shows statistics and lets you change the current configuration for the Trivial File Transfer Protocol (TFTP) server.	*66*
Tunnel	Lets you change the current configuration settings for a tunnel.	*34*
XML	Lets you export XML configuration and status records, and import XML configuration records.	*116*

5: Network Settings

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

This chapter contains the following sections:

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

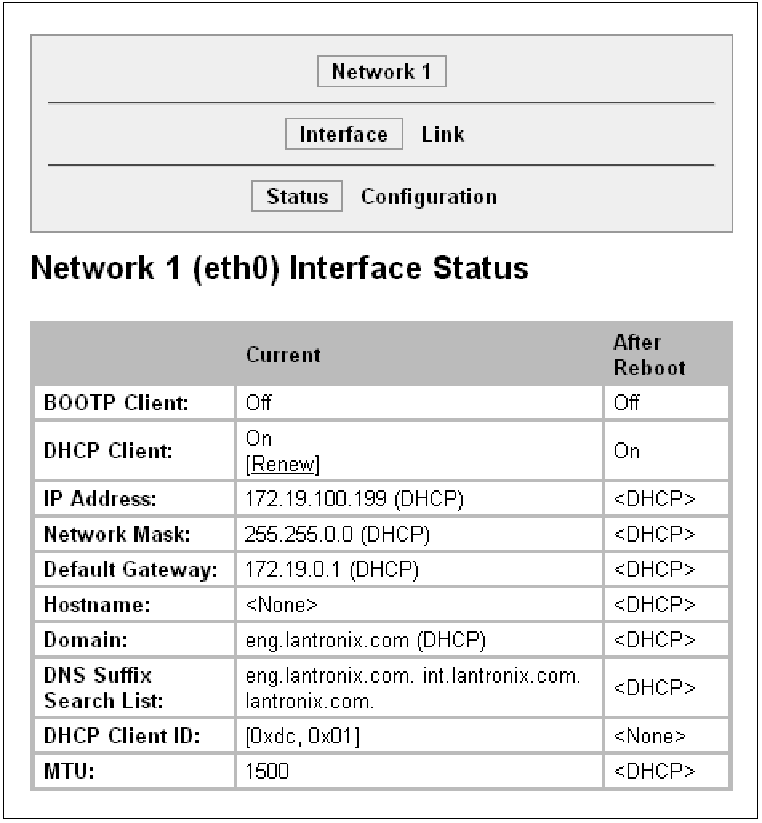
Network 1 (eth0) Interface Status

This page shows the status of the Ethernet network interface.

To view the network interface status:

1. Click **Network** on the menu.
2. Then click **Network 1**, **Interface**, and **Status** at the top of the page. The Network 1 (eth0) Interface Status page appears.

Figure 5-1 Network 1 (eth0) Interface Status



Network 1 (eth0) Interface Status

	Current	After Reboot
BOOTP Client:	Off	Off
DHCP Client:	On [Renew]	On
IP Address:	172.19.100.199 (DHCP)	<DHCP>
Network Mask:	255.255.0.0 (DHCP)	<DHCP>
Default Gateway:	172.19.0.1 (DHCP)	<DHCP>
Hostname:	<None>	<DHCP>
Domain:	eng.lantronix.com (DHCP)	<DHCP>
DNS Suffix Search List:	eng.lantronix.com. int.lantronix.com. lantronix.com.	<DHCP>
DHCP Client ID:	[0xdc, 0x01]	<None>
MTU:	1500	<DHCP>

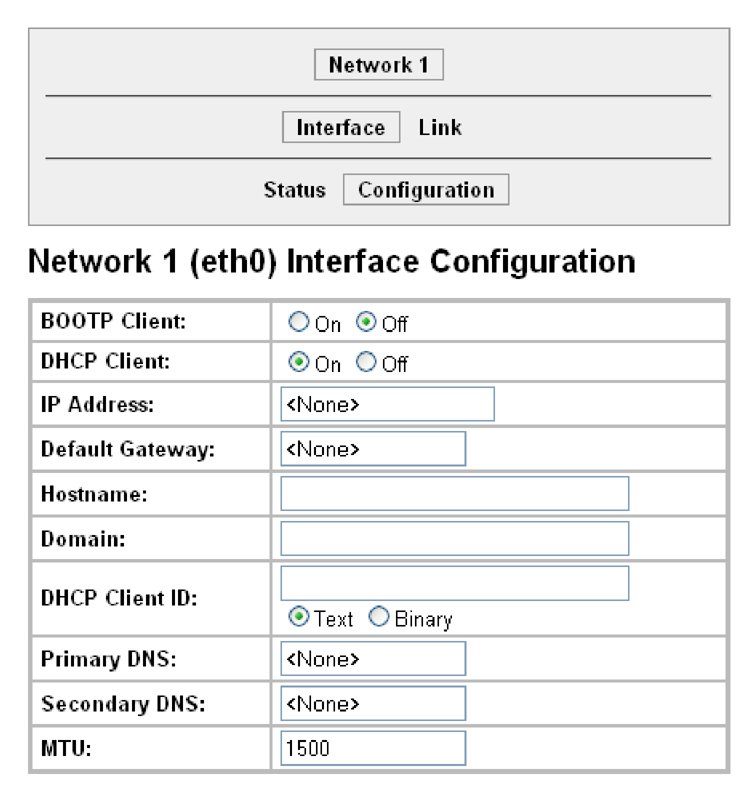
Network 1 (eth0) Interface Configuration

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

To view and configure network interface settings:

1. Click **Network 1 > Interface > Configuration** at the top of the page. The Network 1 (eth0) Interface Configuration page appears.

Figure 5-2 Network 1 (eth0) Interface Configuration



Network 1 (eth0) Interface Configuration

BOOTP Client:	○ On ● Off
DHCP Client:	● On ○ Off
IP Address:	<None>
Default Gateway:	<None>
Hostname:	
Domain:	
DHCP Client ID:	● Text ○ Binary
Primary DNS:	<None>
Secondary DNS:	<None>
MTU:	1500

Note: *MTU is not supported on XPort AR.*

2. Enter or modify the following settings:

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

Network 1 Interface Configuration Settings	Description
BOOTP Client	Select **On** or **Off**. At boot up, the device will attempt to obtain an IP address from a BOOTP server. **Notes:** ◆ *Overrides the configured IP address, network mask, gateway, hostname, and domain.* ◆ *When DHCP is On, the system automatically uses DHCP, regardless of whether BOOTP Client is On.*
DHCP Client	Select **On** or **Off**. At boot up, the device will attempt to lease an IP address from a DHCP server and maintain the lease at regular intervals. *Note: Overrides BOOTP, the configured IP address, network mask, gateway, hostname, and domain.*
IP Address	Enter the device static IP address. You may enter it alone, in CIDR format, or with an explicit mask. The IP address consists of four octets separated by a period and is used if BOOTP and DHCP are both set to **Off**. Changing this value requires you to reboot the device. *Note: When DHCP is enabled, the device tries to obtain an IP address from DHCP. If it cannot, the device uses an AutoIP address in the range of 169.254.xxx.xxx.*
Default Gateway	Enter the IP address of the router for this network. Or, clear the field (appears as **<None>**). This address is only used for static IP address configuration.
Hostname	Enter the device hostname. It must begin with a letter, continue with a sequence of letters, numbers, and/or hyphens, and end with a letter or number.
Domain	Enter the device domain name.
DHCP Client ID	Enter the ID if the DHCP server uses a DHCP ID. The DHCP server's lease table shows IP addresses and MAC addresses for devices. The lease table shows the Client ID, in hexadecimal notation, instead of the device MAC address.
Primary DNS	IP address of the primary name server. This entry is required if you choose to configure DNS (Domain Name Server) servers.
Secondary DNS	IP address of the secondary name server.

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

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

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

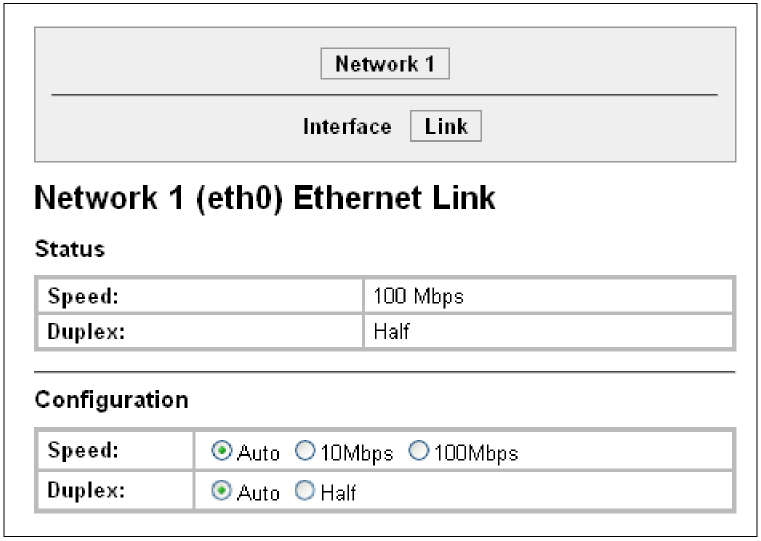
Network 1 Ethernet Link

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

To view and configure the Ethernet link:

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

Figure 5-4 Network 1 Ethernet Link



Network 1 (eth0) Ethernet Link

Status

Speed:	100 Mbps
Duplex:	Half

Configuration

Speed:	● Auto ○ 10Mbps ○ 100Mbps
Duplex:	● Auto ○ Half

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

2. Enter or modify the following settings:

Table 5-5 **Network 1 Ethernet Link**

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

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

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

6: Line and Tunnel Settings

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

- Line Settings
- Tunnel Settings

Note: The number of lines and tunnels available for viewing and configuration differ between Lantronix DeviceLinx products. The screenshots in this manual represent one line and tunnel, as available, for example, on an XPort Pro and EDS1100. However, other device networking products (such as EDS2100, EDS4100, XPort AR, and EDS8/16/32PR) support additional lines and tunnels.

Line Settings

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

The following sub-menus can be used:

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

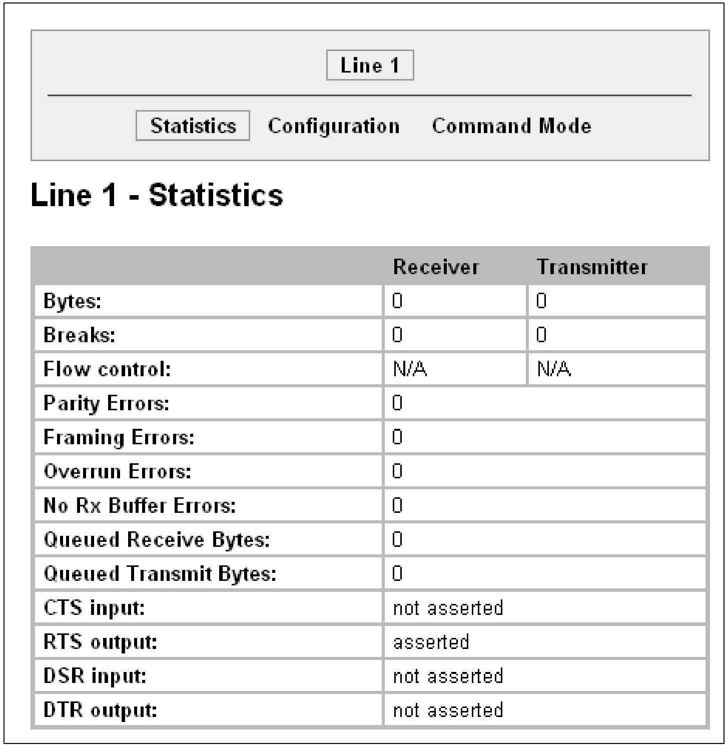
The following sections describe the steps to view and configure Line 1 settings. These instructions also apply to additional line menu options.

Line Statistics

This read-only web 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 Statistics page appears.

Figure 6-1 Line 1 Statistics



Line 1 - Statistics

	Receiver	Transmitter
Bytes:	0	0
Breaks:	0	0
Flow control:	N/A	N/A
Parity Errors:	0	
Framing Errors:	0	
Overrun Errors:	0	
No Rx Buffer Errors:	0	
Queued Receive Bytes:	0	
Queued Transmit Bytes:	0	
CTS input:	not asserted	
RTS output:	asserted	
DSR input:	not asserted	
DTR output:	not asserted	

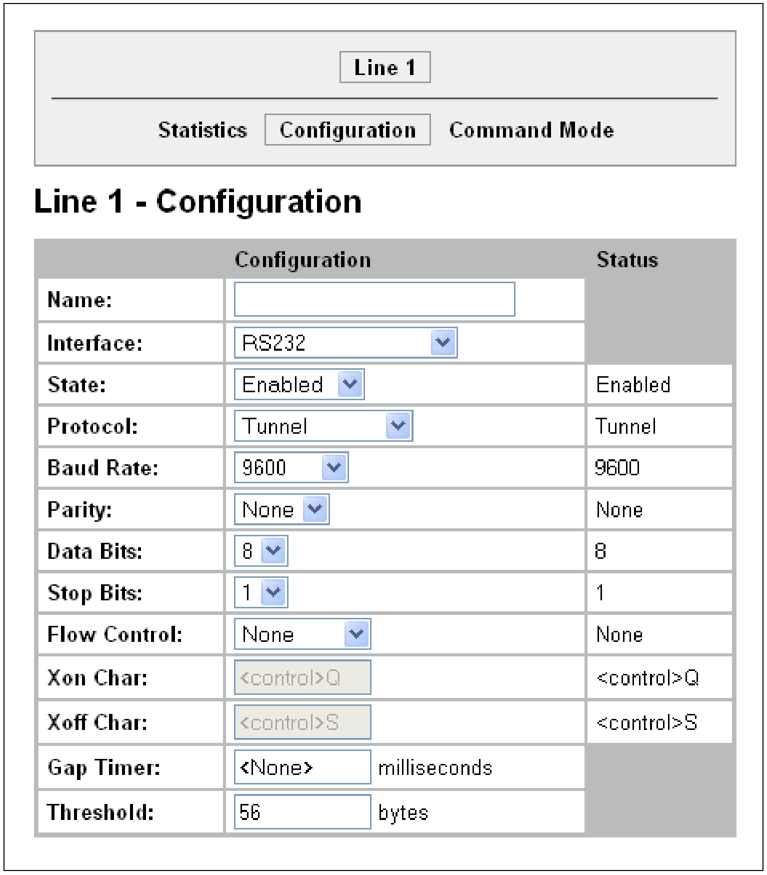
Line Configuration

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

To configure Line 1:

1. Click **Line 1 > Configuration** at the top of the page. The Line 1 Configuration page appears.

Table 6-2 **Line 1 Configuration**



Line 1 - Configuration

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

2. Enter or modify the following settings:

Table 6-3 **Line 1 Configuration**

Line - Configuration Settings	Description
Name	If the Terminal Login Menu feature is being used, enter the name for the line. Leaving this field blank will disable this line from appearing in the Terminal Login Menu. The default Name is blank. See *Terminal and Host Settings on page 50* for related configuration information.
Interface	Select the interface type from the drop-down menu. The default is RS232.
State	Indicates whether the current line is enabled. To change the status, select Enabled or Disabled from the drop-down menu.
Protocol	Select the protocol from the drop-down menu. The default is Tunnel.
Baud Rate	Select the baud rate from the drop-down menu. The default is 9600.

Line - Configuration Settings (continued)	Description
Parity	Select the parity from the drop-down menu. The default is None.
Data Bits	Select the number of data bits from the drop-down menu. The default is 8.
Stop Bits	Select the number of stop bits from the drop-down menu. The default is 1.
Flow Control	Select the flow control from the drop-down menu. The default is None.
Xon Char	Specify the character to use to start the flow of data when Flow Control is set to Software. Prefix a decimal character with \ or a hexadecimal character with 0x, or provide a single printable character. The default Xon char is 0x11.
Xoff Char	Specify the character to use to stop the flow of data when Flow Control is set to Software. Prefix a decimal character with \ or a hexadecimal character with 0x, or provide a single printable character. The default Xoff char is 0x13.
Gap Timer	The driver forwards received serial bytes after the **Gap Timer** delay from the last character received. By default, the delay is four character periods at the current baud rate (minimum 1 ms).
Threshold	The driver will also forward received characters after **Threshold** bytes have been received.

3. Click **Submit.**
4. Repeat above steps as desired, according to additional line(s) available for your product.

Line Command Mode

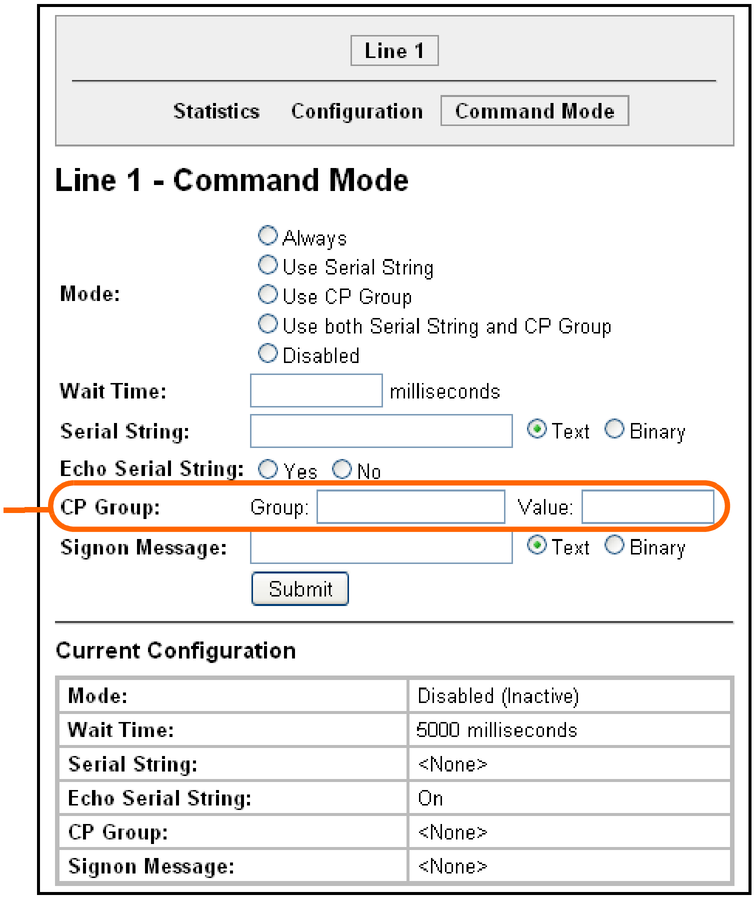
Setting Command Mode enables the CLI on the serial line.

To configure Line 1 Command Mode:

1. Click **Line 1 > Command Mode** at the top of the page. The Line 1 Command Mode page appears.

Note: *The* **CP Group** *option displayed in the screenshot is only supported in XPort Pro and XPort AR.*

Figure 6-4 Line 1 Command Mode



Line 1 - Command Mode

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

Wait Time: milliseconds

Serial String: ● Text ○ Binary

Echo Serial String: ○ Yes ○ No

CP Group: Group: Value:

Signon Message: ● Text ○ Binary

Current Configuration

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

2. Enter or modify the following settings:

Table 6-5 **Line 1 Command Mode**

Line – Command Mode 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. ◆ **Use CP Group** = enables Command Mode based on the status of a CP Group. When the value matches the current value of the group, Command Mode is enabled on the serial line. ◆ **Use both Serial String and CP Group** = the serial string and the value of the CP group must be matched to enable Command Mode. ◆ **Disabled** = turns off Command Mode.
Wait Time	Enter the wait time for the serial string during boot-up in milliseconds.

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

3. Click **Submit.**

Tunnel Settings

Note: The number of lines and tunnels available for viewing and configuration differ between Lantronix DeviceLinx products. The screenshots in this manual represent one line and tunnel, as available, for example, on an XPort Pro and EDS1100. However, other device networking products (such as EDS2100, EDS4100, XPort AR, and EDS8/16/32PR) support additional lines and tunnels.

Tunneling allows serial devices to communicate over a network, without “being aware” of the devices which establish the network connection between them. Tunneling parameters are configured using the Web Manager or Command Mode Tunnel Menu. See *Configuration Using Web Manager (on page 21)* or the XPort AR Command Reference for the full list of commands.

The XPort 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 another serial port.

- **Connect Mode:** the XPort 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 XPort 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 XPort AR Disconnect Mode observes the defined event occur, it will disconnect both Accept Mode and Connect Mode connections on that port.

When any character comes in through the serial port, it gets copied to both the Connect Mode connection and the Accept Mode connection (if both are active).

You can view statistics and configure two tunnels by using the Tunnel web page. When you click Tunnel from the Main Menu, Tunnel 1 fields display. To go to Tunnel 2, click the Tunnel 2 button.

There are six sub-menus listed at the top of the Tunnel web page that you can use as follows:

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

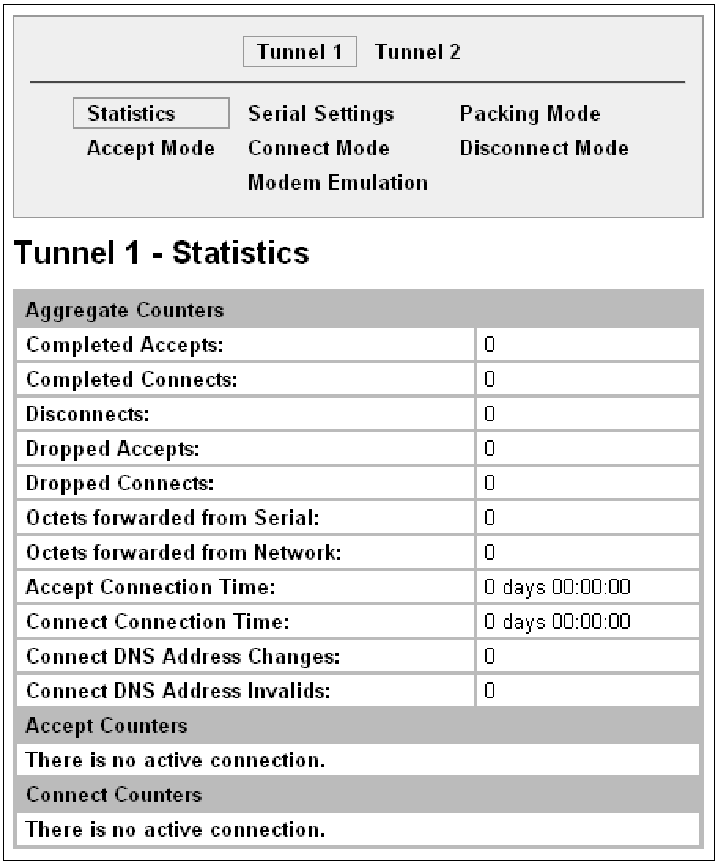
Tunnel – Statistics

Displays statistics for the available lines. For example, Completed Accepts, Completed Connects, Disconnects, Dropped Accepts, Dropped Connects, etc. The XPort AR logs statistics for tunneling. The **Dropped** statistic shows connections ended by the remote location. The **Disconnects** statistic shows connections ended by the XPort AR.

To display the tunnel statistics, perform the following steps.

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

Figure 6-6 Tunnel 1 Statistics



Tunnel 1 - Statistics

Aggregate Counters	
Completed Accepts:	0
Completed Connects:	0
Disconnects:	0
Dropped Accepts:	0
Dropped Connects:	0
Octets forwarded from Serial:	0
Octets forwarded from Network:	0
Accept Connection Time:	0 days 00:00:00
Connect Connection Time:	0 days 00:00:00
Connect DNS Address Changes:	0
Connect DNS Address Invalids:	0
Accept Counters	
There is no active connection.	
Connect Counters	
There is no active connection.	

Tunnel – Serial Settings

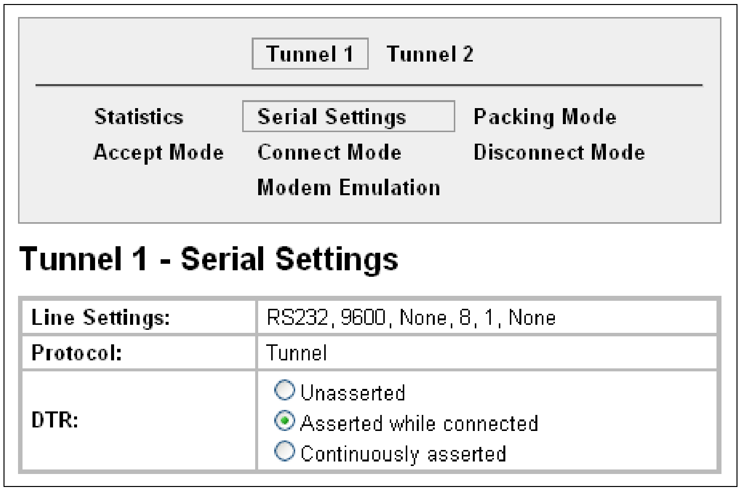
Serial line settings are configurable for the corresponding serial line of the selected tunnel. Configure the buffer size to change the maximum amount of data the serial port stores. For any active connection, the device sends the data in the buffer.

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

To configure serial settings:

1. Click **Tunnel > Serial Settings** at the top of the page. The Tunnel 1 Serial Settings page appears.

Figure 6-7 Tunnel 1 Serial Settings



Tunnel 1 - Serial Settings

Line Settings:	RS232, 9600, None, 8, 1, None
Protocol:	Tunnel
DTR:	○ Unasserted ● Asserted while connected ○ Continuously asserted

2. View or modify the following settings:

Table 6-8 **Tunnel - Serial Settings**

Tunnel - Serial Settings	Description
Line Settings *(display only)*	Current serial settings for the line.
Protocol *(display only)*	The protocol being used on the line. In this case, Tunnel.
DTR	Select when to assert DTR. ◆ **Unasserted** = never asserted ◆ **Asserted while connected** = asserted whenever either a connect or an accept mode tunnel connection is active. ◆ **Continuously asserted** = asserted regardless of the status of a tunnel connection.

3. Click **Submit.**

Tunnel – Packing Mode

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

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

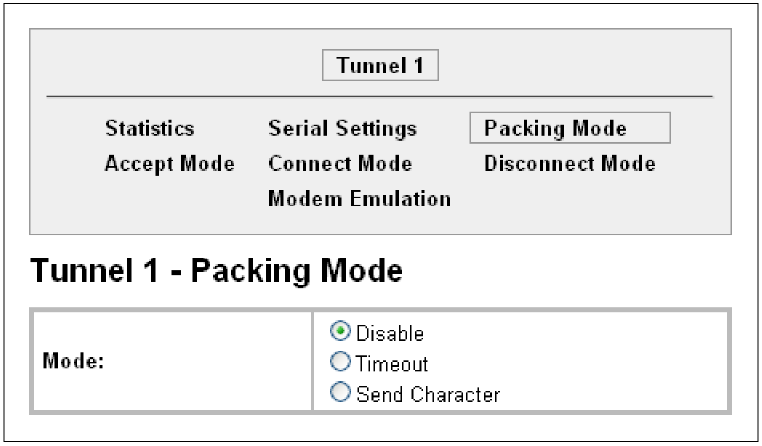
The timeout field is used to force a packet to be sent after a maximum time. The packet is sent even if the threshold value is not reached.

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

To configure the Tunnel Packing Mode:

1. Select **Tunnel > Packing Mode** at the top of the page. The Tunnel 1 Packing Mode page appears. Depending on the Mode selection, different configurable parameters are presented to the user. The following figures show the display for each of the three packing modes.

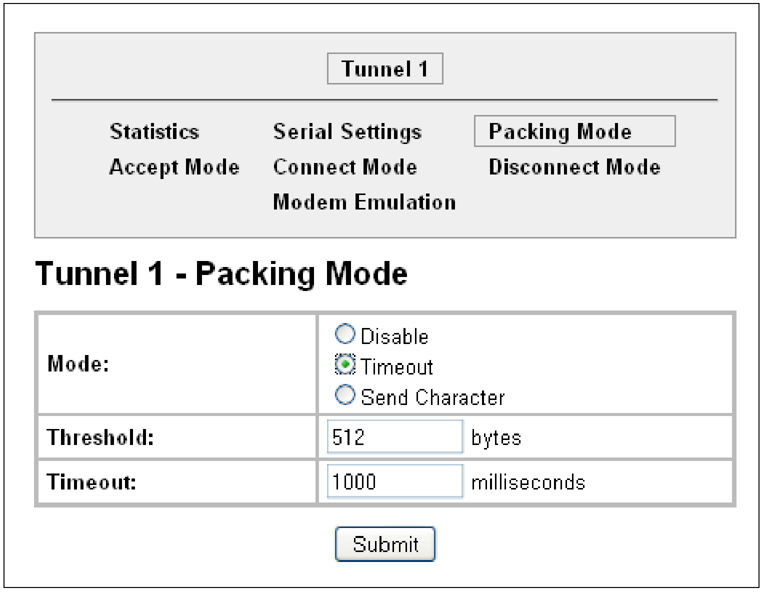
Figure 6-9 Tunnel 1 Packing Mode (Mode = Disable)



Tunnel 1 - Packing Mode

Mode:	● Disable ○ Timeout ○ Send Character

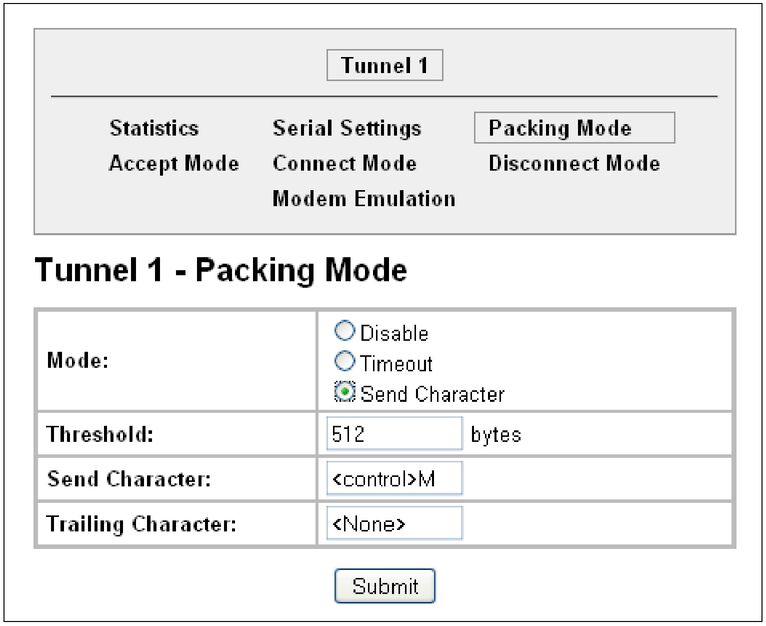
Figure 6-10 Tunnel 1 Packing Mode (Mode = Timeout)



Tunnel 1 - Packing Mode

Mode:	○ Disable ● Timeout ○ Send Character
Threshold:	512 bytes
Timeout:	1000 milliseconds

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



Tunnel 1 - Packing Mode

Mode:	○ Disable ○ Timeout ● Send Character
Threshold:	512 bytes
Send Character:	<control>M
Trailing Character:	<None>

2. Enter or modify the following settings:

Table 6-12 **Tunnel Packing Mode**

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

3. Click **Submit.**

Tunnel – Accept Mode

Controls how a tunnel behaves when a connection attempt originates from the network. In Accept Mode, the XPort AR waits for a connection from the network. The configurable local port is the port the remote device connects to for this connection. There is no remote port or address. The default local port is 10001 for serial port 1 and increases sequentially for each additional serial port, if supported.

Accept Mode supports the following protocols:

- SSH (the XPort 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.
- SSL
- TCP
- AES encryption over TCP
- Telnet (The XPort AR supports IAC codes. It drops the IAC codes when Telnetting and does not forward them to the serial port).

Accept Mode has the following states:

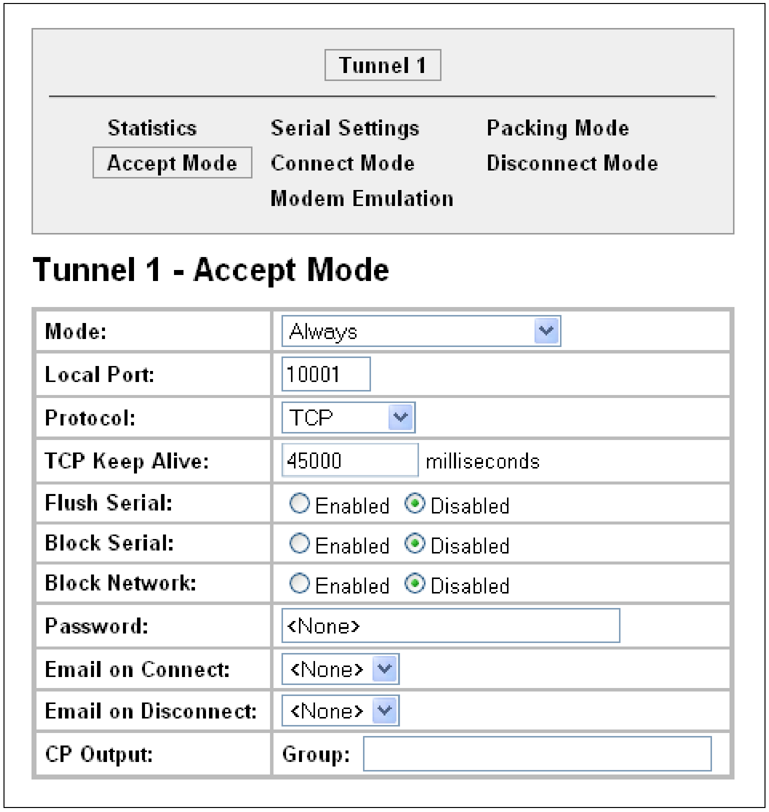
- Disabled (never a connection)
- Enabled (always listening for a connection)
- Active if it receives any character from the serial port
- Active if it receives a specific (configurable) character from the serial port (same start character as Connect Mode’s start character)
- Modem control signal
- Modem emulation

To configure the tunnel’s Accept Mode:

1. Click **Tunnel > Accept Mode** at the top of the page. The Tunnel 1 Accept Mode page appears.

Note: *The* **CP Output** *option displayed in the screenshot is only supported in XPort Pro and XPort AR.*

Figure 6-13 Tunnel 1 Accept Mode



Tunnel 1 - Accept Mode

Mode:	Always
Local Port:	10001
Protocol:	TCP
TCP Keep Alive:	45000 milliseconds
Flush Serial:	○ Enabled ● Disabled
Block Serial:	○ Enabled ● Disabled
Block Network:	○ Enabled ● Disabled
Password:	<None>
Email on Connect:	<None>
Email on Disconnect:	<None>
CP Output:	Group:

2. Enter or modify the following settings:

Table 6-14 **Tunnel Accept Mode**

Tunnel - Accept Mode Settings	Description
Mode	Select the method used to start a tunnel in Accept mode. Choices are: ◆ **Disabled** = do not accept an incoming connection. ◆ **Always** = 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. Additional tunnels, if supported, increase sequentially.
Protocol	Select the protocol type for use with Accept Mode. The default protocol is TCP. If you select TCP AES you will need to configure the AES keys.
TCP Keep Alive	Enter the time, in seconds, the device waits during a silent connection before checking if the currently connected network device is still on the network. If the unit then gets no response after 8 attempts, it drops that connection.

Tunnel - Accept Mode Settings (continued)	Description
Flush Serial Data	Select Enabled to flush the serial data buffer on a new connection.
Block Serial Data	Select On to block, or not tunnel, serial data transmitted to the device.
Block Network	Select On to block, or not tunnel, network data transmitted to the device.
Password	Enter a password that clients must send to the device within 30 seconds from opening a network connection to enable data transmission. The password can have up to 31 characters and must contain only alphanumeric characters and punctuation. When set, the password sent to the device must be terminated with one of the following: (a) 0x0A (LF), (b) 0x00, (c) 0x0D 0x0A (CR LF), or (d) 0x0D 0x00.
Email on Connect	Select whether the device sends an email when a connection is made. Select None if you do not want to send an email. Otherwise, select the Email profile to use for sending.
Email on Disconnect	Select whether the device sends an email when a connection is closed. Select None if you do not want to send an email. Otherwise, select the Email profile to use for sending.

3. Click **Submit.**
4. Repeat these steps to configure additional tunnels as applicable.

Tunnel – Connect Mode

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

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

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

Connect Mode supports the following protocols:

- **TCP**
- **AES encryption over TCP and UDP**

  When setting AES encryption, both the encrypt key and the decrypt key must be specified. The encrypt key is used for data sent out. The decrypt key is used for receiving data. Both of the keys may be set to the same value.
- **SSH**

  To configure SSH, the SSH client username must be configured. In Connect Mode, the XPort AR is the SSH client. Ensure the XPort AR SSH client username is configured on the remote SSH server before using it with the XPort AR.
- **SSL**
- **UDP**

  Is only available in Connect Mode because it is a connectionless protocol. For Connect Mode using UDP, the XPort AR accepts packets from any device on the network. It will send packets to the last device that sent it packets.
- **Telnet**

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

There are six different connect modes:

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

Note: *While in the “Any Character” or “Start Character” connection modes, the XPort 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 another character or the start character again (depending on the configured setting).*

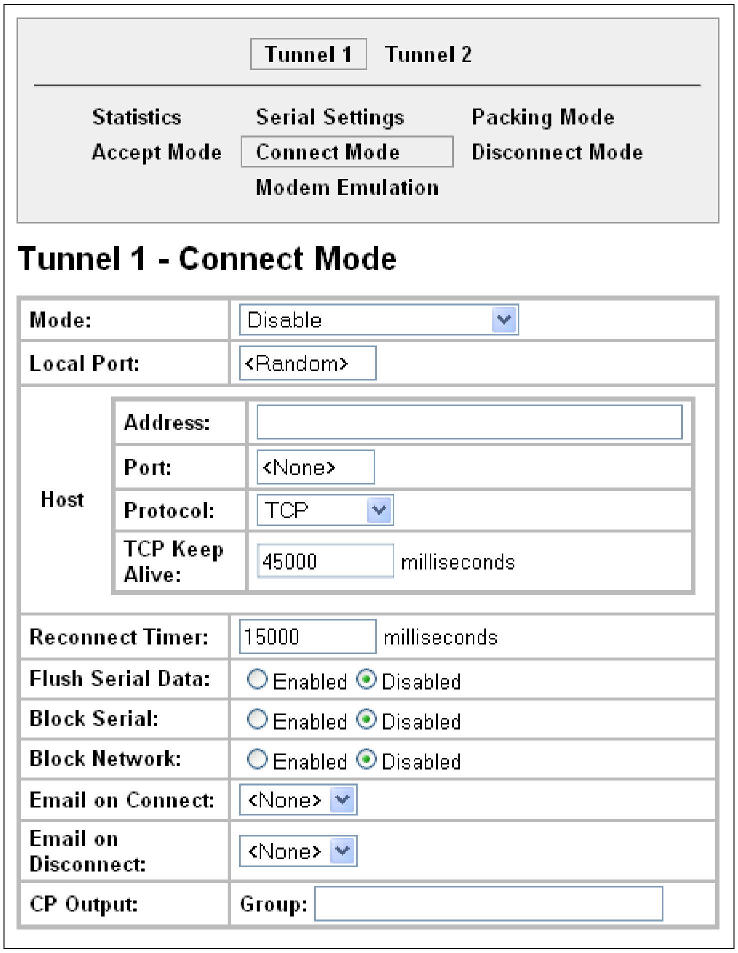
- **Modem Control Asserted**
  A connection is attempted when the modem control pin is asserted in the serial line.
- **Modem Emulation**
  A connection is attempted by an ATD command.

To configure Tunnel 1 Connect Mode:

1. Select **Tunnel > Connect Mode** at the top of the page. The Tunnel 1 Connect Mode page appears.

Note: The **CP Output** *option displayed in the screenshot is only supported in XPort Pro and XPort AR.*

Figure 6-15 Tunnel 1 Connect Mode



Tunnel 1 - Connect Mode

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

2. Enter or modify the following settings:

Table 6-16 **Tunnel Connect Mode**

Tunnel – Connect Mode Settings	Description
Mode	Select the method to be used to attempt a connection to a remote host or device. Choices are: ◆ **Always** = a connection is attempted until one is made. If the connection gets disconnected, the XPort AR retries until it makes a connection. (default) ◆ **Disable** = an outgoing connection is never attempted. ◆ **Any Character** = a connection is attempted when any character is read on the serial line. ◆ **Start Character** = a connection is attempted when the start character for the selected tunnel is read on the serial line. ◆ **Modem Control Asserted** = a connection is attempted as long as the Modem Control pin (DSR) is asserted, until a connection is made. ◆ **Modem Emulation** = a connection is attempted when triggered by modem emulation AT commands.
Local Port	Enter the port for use as the local port. A random port is selected by default. Once you have configured a number, click the Random link in the Current Configuration to switch back to random.
Host *Note: If security is a concern, it is highly recommended that SSH be used. When using SSH, both the SSH Server Host Keys and SSH Server Authorized Users must be configured.*	◆ **Address** = Enter the remote Host Address as an IP address or DNS name. It designates the address of the remote host to connect to. Displays configured IP address or DNS address, used only if VIP is disabled. ◆ **Port** = Enter the port for use as the Host Port. It designates the port on the remote host to connect to. Displays configured Port. ◆ **Protocol** = Select the protocol type for use with Connect Mode. The default protocol is TCP. Additional fields may need to be completed depending on protocol chosen for the host.: ➢ For **SSH**, also enter an **SSH Username**. ➢ For **SSL**, also select Enabled or Disabled for **Validate Certificate**. ➢ For **SSL**, **TCP**, **TCP AES** and **Telnet**, use the **TCP Keep Alive** field to adjust the value. ➢ For **TCP AES**, enter the **AES Encrypt** and **AES Decrypt Keys**. Both of keys may be set to the same value. ➢ For **UDP**, there are no additional fields to complete. In this mode, the device accepts packets from any device on the network and sends packets to the last device that sent it packets. ➢ For **UDP AES**, enter the **AES Encrypt** and **AES Decrypt Keys**. ◆ **SSH Username** = Displays configured username, used only if SSH protocol is selected. ◆ **TCP Keep Alive** = Default is 45000 milliseconds. Enter zero to disable and blank the value to restore the default. ◆ **AES Encrypt/Decrypt Key** = Displays presence of key, used only if protocol with AES is selected.

Tunnel – Connect Mode Settings (continued)	Description
Reconnect Timer	Enter the reconnect time in milliseconds. The device attempts to reconnect after this amount of time after failing a connection or exiting an existing connection. This behavior depends upon the Disconnect Mode. ***Note:*** ◆ *When you configure* **Tunnel - Connect Mode***, you can specify a number of milliseconds to attempt to reconnect after a dropped connection has occurred. The default is 1500 milliseconds.* ◆ *The* ***Reconnect Timer*** *only applies if a* **Disconnect Mode** *is configured. With a* **Disconnect Mode** *set, the device server maintains a connection until the disconnect mode condition is met (at which time the device server closes the connection). If the tunnel is dropped due to conditions beyond the device server, the device server attempts to re-establish a failed connection when the specified reconnect interval reaches its limit.* ◆ *Any network-side disconnect is considered an error and a reconnect is attempted without regard to the* **Connect Mode** *settings. Simultaneous* **Connect Mode** *connections require some* **Disconnect Mode** *configurations or the connections will never terminate. See Tunnel – Disconnect Mode on page 46 for more information about the parameters.* ◆ *If* **Disconnect Mode** *is disabled and the network connection is dropped, then the re-establishment of a tunnel connection is governed by the configured* **Connect Mode** *settings.*
Flush Serial Data	Select whether to flush the serial line when a connection is made. Choices are: ◆ **Enabled** = flush the serial line when a connection is made. ◆ **Disabled** = do not flush the serial line. (default)
Block Serial	Select **Enabled** to block (not tunnel) serial data transmitted to the device. This is a debugging tool that causes serial data sent to the device to be ignored.
Block Network	Select **Enabled** to block (not tunnel) network data transmitted to the device. This is a debugging tool that causes network data sent to the device to be ignored.
Email on Connect	Select whether the device sends an email when a connection is made. Select None if you do not want to send an email. Otherwise, select the Email profile to use.
Email on Disconnect	Select whether the device sends an email when a connection is closed. Select None if you do not want to send an email. Otherwise, select the Email profile to use.
CP Output	Identifies a CP or CP Group whose value should change when a connection is established and when it is dropped. ◆ **Connection value**—Specifies the value to set the CP Group to when a connection is established. ◆ **Disconnection value**—Specifies the value to set the CP Group to when the connection is closed.

3. Click **Submit.** The host is configured.

Tunnel – Disconnect Mode

Relates to the disconnect of a tunnel. Disconnect Mode ends Accept Mode and Connect Mode connections. When disconnecting, the XPort AR shuts down connections gracefully.

The following settings end a connection:

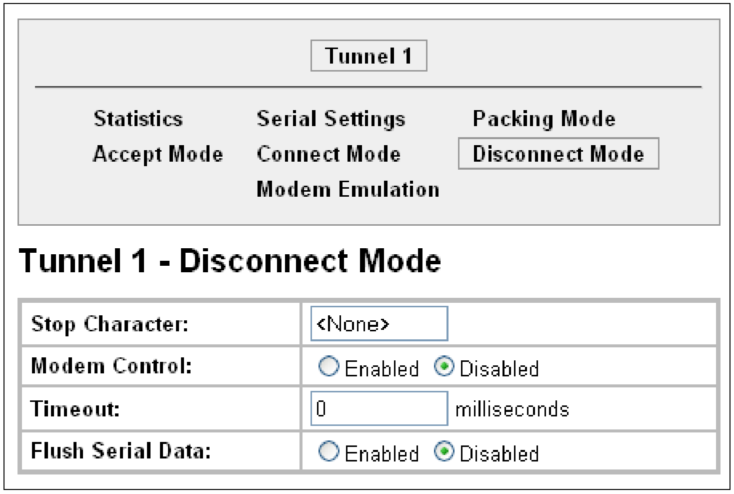
- The XPort AR receives the stop character.
- The timeout period has elapsed and no activity is going in or out of the XPort AR. Both Accept Mode and Connect Mode must be idle for the time frame.
- The XPort AR observes the modem control inactive setting.

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

To configure the tunnel Disconnect Mode:

1. Click **Tunnel > Disconnect Mode** at the top of the page. The Tunnel 1 Disconnect Mode page appears.

Figure 6-17 Tunnel 1 Disconnect Mode



Tunnel 1 - Disconnect Mode

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

2. Enter or modify the following settings:

Table 6-18 **Tunnel Disconnect Mode**

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

3. Click **Submit.**

Tunnel – Modem Emulation

A tunnel in Connect Mode can be initiated using modem commands incoming from the Serial Line. This page enables you to configure the modem emulation settings when you select Modem Emulation as the Tunnel Connect Mode type.

The Modem Emulation Command Mode supports the standard AT command set. For a list of available commands from the serial or Telnet login, enter **AT?**. Use **ATDT**, **ATD**, and **ATDP** to establish a connection. All of these commands behave like a modem. For commands that are valid but not applicable to the XPort AR, an “OK” message is sent (but the command is silently ignored).

The XPort 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.

The following table lists and describes the available commands.

Table 6-19 **Modem Emulation Commands and Descriptions**

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

Table 6-19 **Modem Emulation Commands and Descriptions (continued)**

Command (continued)	Description
A/	Repeat last valid command.

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

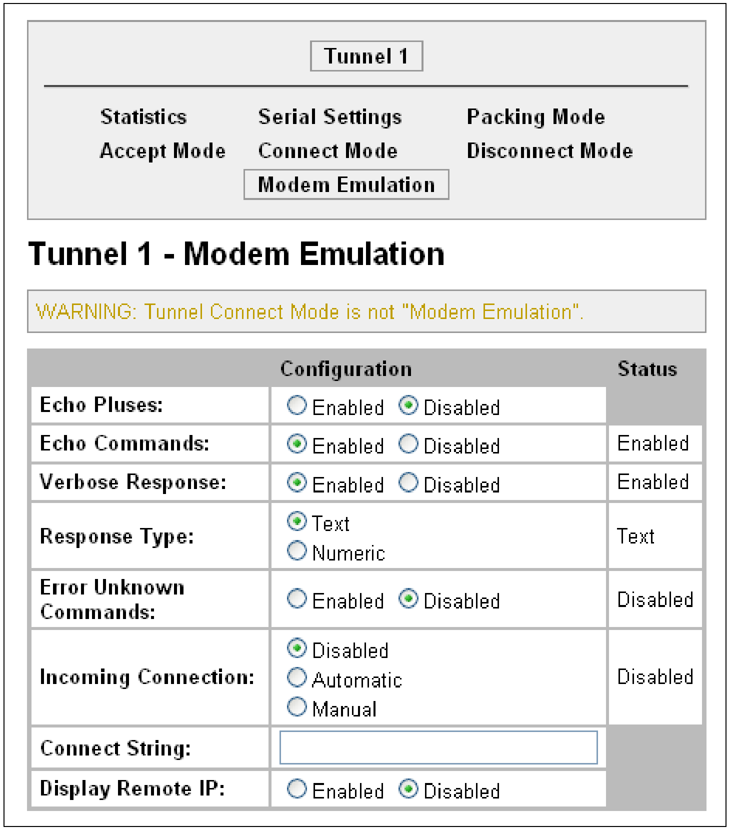
For ATDT and ATDP commands less than 255 characters, the XPort AR replaces the last segment of the IP address with the configured Connect Mode remote station address. It is possible to use the last two segments also, if they are under 255 characters. For example, if the address is 100.255.15.5, entering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

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

To configure modem emulation:

1. Select **Tunnel > Modem Emulation** at the top of the page. The Tunnel 1 Modem Emulation page appears.

Figure 6-20 Tunnel 1 Modem Emulation



Tunnel 1 - Modem Emulation

WARNING: Tunnel Connect Mode is not "Modem Emulation".

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

2. Enter or modify the following settings:

Table 6-21 **Tunnel Modem Emulation**

Tunnel- Modem Emulation Settings	Description
Echo Pluses	Select **Enabled** to echo **+++** when entering modem Command Mode.
Echo Commands	Select **Enabled** to echo the modem commands to the console.
Verbose Response	Select **Enabled** to send modem response codes out on the serial line.
Response Type	Select the type of response code: **Text** or **Numeric**.
Error Unknown Commands	Select whether an **ERROR** or **OK** response is sent in reply to unrecognized AT commands. Choices are: ◆ **Enabled** = **ERROR** is returned for unrecognized AT commands. ◆ **Disabled** = **OK** is returned for unrecognized AT commands. Default is **Disabled**.
Incoming Connection	Select whether Incoming Connection requests will be disabled, answered automatically, or answered manually. Default is **Disabled**.
Connect String	Enter the connect string. This modem initialization string prepares the modem for communications. It is a customized string sent with the “CONNECT” modem response code.
Display Remote IP	Selects whether the incoming RING sent on the Serial Line is followed by the IP address of the caller. Default is **Disabled**.

3. Click **Submit.**

7: Terminal and Host Settings

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

- *Terminal Settings*
- *Host Configuration*

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

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

Terminal Settings

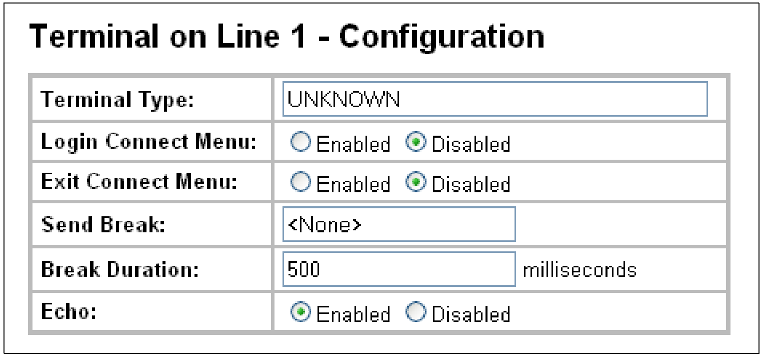
This page shows configuration settings for each terminal connection method. You can configure whether each serial line or the telnet/SSH server presents a CLI or a Login Connect menu when a connection is made.

Line Terminal Configuration

To configure a line to support an attached terminal:

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

Figure 7-1 Terminal on Line Configuration



Terminal on Line 1 - Configuration

Terminal Type:	UNKNOWN
Login Connect Menu:	○ Enabled ● Disabled
Exit Connect Menu:	○ Enabled ● Disabled
Send Break:	<None>
Break Duration:	500 milliseconds
Echo:	● Enabled ○ Disabled

2. Enter or modify the following settings:

Table 7-2 **Terminal on Line 1 Configuration**

Terminal on Line Configuration Settings	Description
Terminal Type	Enter text to describe the type of terminal. The text will be sent to a host via IAC. ***Note:*** *IAC means, "interpret as command." It is a way to send commands over the network such as* **send break** *or* **start echoing**.
Login Connect Menu	Select the interface to display when the user logs in. Choices are: ◆ **Enabled** = shows the Login Connect Menu. ◆ **Disabled** = shows the CLI
Exit Connect Menu	Select whether to display a choice for the user to exit the Login Connect Menu and reach the CLI. Choices are: ◆ **Enabled** = a choice allows the user to exit to the CLI. ◆ **Disabled** = there is no exit to the CLI.
Send Break	Enter a Send Break control character, e.g., <control> Y, or blank to disable. When the Send Break control character is received from the network on its way to the serial line, it is not sent to the line; instead, the line output is forced to be inactive (the break condition).
Break Duration	Enter how long the break should last in milliseconds.
Echo	Applies only to Connect Mode Telnet connections, not to Accept Mode. Only disable **Echo** if your terminal echoes, in which case you will see double of each character typed.

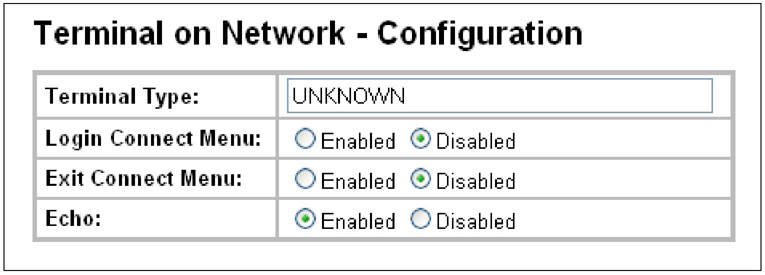
3. Click **Submit** to save changes.
4. Repeat these steps to configure additional lines as necessary.

Network Terminal Configuration

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

1. Click **Terminal > Network** at the top of the page. Configuration is automatically selected. The Terminal on Network Configuration page appears.

Figure 7-3 Terminal on Network Configuration



Terminal on Network - Configuration

Terminal Type:	UNKNOWN
Login Connect Menu:	○ Enabled ● Disabled
Exit Connect Menu:	○ Enabled ● Disabled
Echo:	● Enabled ○ Disabled

2. Enter or modify the following settings:

Table 7-4 **Terminal on Network Configuration**

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

3. Click **Submit** to save changes.

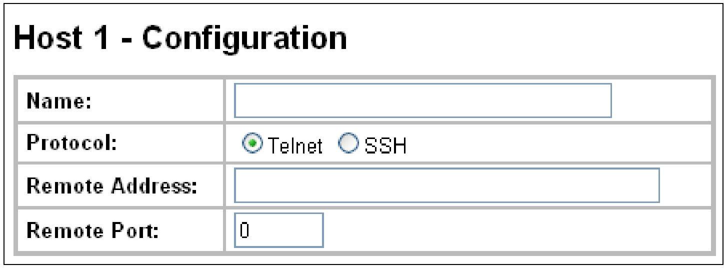
Host Configuration

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

To configure a remote host, perform the following steps.

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

Figure 7-5 Host Configuration



Host 1 - Configuration

Name:	
Protocol:	● Telnet ○ SSH
Remote Address:	
Remote Port:	0

2. Enter or modify the following settings:

***Table 7-6* Host Configuration**

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

3. Click **Submit** to save changes.
4. Repeat these steps to configure additional hosts, as needed.

8: Configurable Pin Manager

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

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

This chapter contains the following sections:

- *Overview*
- *CPM: CP (Configurable Pins)*
- *CPM: Groups*

Overview

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

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

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

Default Groups

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

Custom Groups

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

CPM: CP (Configurable Pins)

Each CP is associated with an external hardware pin. CPs can trigger an outside event, like sending an email message or starting Command Mode on a serial Line.

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

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

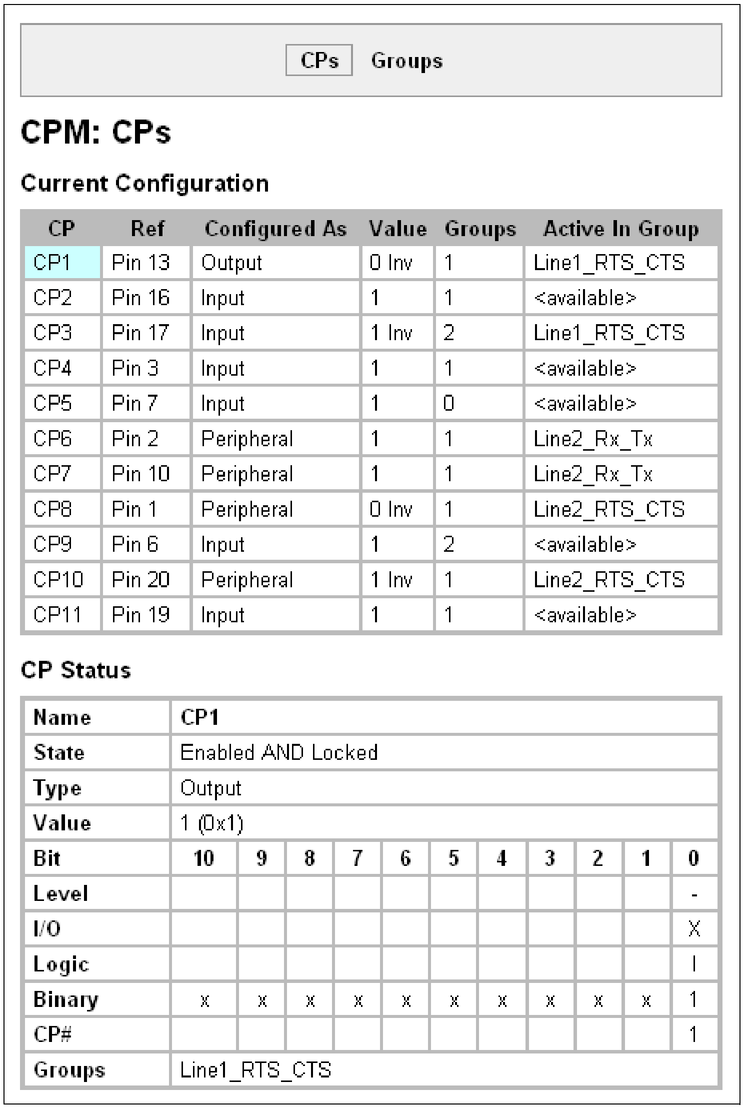
- Can be in any number of groups.
- Can be only in one active group. Two groups with the same CP cannot be enabled at the same time.
- Becomes locked and is not configurable if it is in an enabled group. Disable the group to change the CP configuration.

When you are ready to permanently configure the CPs, use the CPM Groups web page. See CPM: Groups on page 57.

View CPs

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

Figure 8-1 CPM: CPs



CPM: CPs

Current Configuration

CP	Ref	Configured As	Value	Groups	Active In Group
CP1	Pin 13	Output	0 Inv	1	Line1_RTS_CTS
CP2	Pin 16	Input	1	1	<available>
CP3	Pin 17	Input	1 Inv	2	Line1_RTS_CTS
CP4	Pin 3	Input	1	1	<available>
CP5	Pin 7	Input	1	0	<available>
CP6	Pin 2	Peripheral	1	1	Line2_Rx_Tx
CP7	Pin 10	Peripheral	1	1	Line2_Rx_Tx
CP8	Pin 1	Peripheral	0 Inv	1	Line2_RTS_CTS
CP9	Pin 6	Input	1	2	<available>
CP10	Pin 20	Peripheral	1 Inv	1	Line2_RTS_CTS
CP11	Pin 19	Input	1	1	<available>

CP Status

Name	CP1										
State	Enabled AND Locked										
Type	Output										
Value	1 (0x1)										
Bit	**10**	**9**	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**0**
Level											-
I/O											X
Logic											I
Binary	x	x	x	x	x	x	x	x	x	x	1
CP#											1
Groups	Line1_RTS_CTS										

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

Table 8-2 **CPM CPs Current Configuration**

CPM – CPs Current Configuration	Description
CP	Indicates the configurable pin number.
Ref	Indicates the hardware pin number associated with the CP.
Configured As	Shows the CP configuration. A CP configured as **Input** is set to read input. A CP configured as **Output** drives data out of the device.
Value	Indicates the current status of the CP: ◆ **1** = asserted ◆ **0** = de-asserted ◆ **Inv** = the CP logic is inverted
Groups	Indicates the number of groups in which the CP is a member.
Active In Group	Shows the group in which the CP is active. A CP can be a member of several groups. However, it may only be active in one group.

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

Table 8-3 **CPM CPs Status**

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

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

To change a CP output value:

1. Select the CP number (in CP column) from the current configuration table.
2. Enter the CP value in the CP Status table.

3. Click **Set**. The changed CP value appears in the current configuration table.

To change a CP configuration:

1. Select the CP number (in CP column) from the current configuration table.
2. Select the CP configuration from the **Type** drop-down list in the CP Status table.
3. (If necessary) Select the **Assert Low** checkbox.
4. Click **Change**.

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

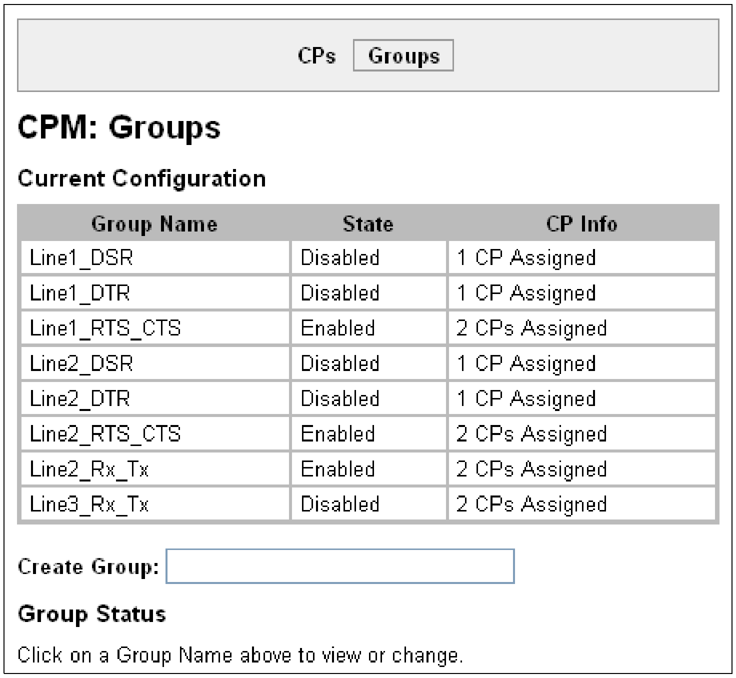
CPM: Groups

The CP Groups page allows for the adding, removing and managing of CP groups. Groups can be created or deleted. CPs can be added to or removed from groups. A group, based on its state, can trigger outside events such as sending email messages. Only an enabled group can be a trigger.

View Groups

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

Figure 8-4 CPM: Groups



CPM: Groups

Current Configuration

Group Name	State	CP Info
Line1_DSR	Disabled	1 CP Assigned
Line1_DTR	Disabled	1 CP Assigned
Line1_RTS_CTS	Enabled	2 CPs Assigned
Line2_DSR	Disabled	1 CP Assigned
Line2_DTR	Disabled	1 CP Assigned
Line2_RTS_CTS	Enabled	2 CPs Assigned
Line2_Rx_Tx	Enabled	2 CPs Assigned
Line3_Rx_Tx	Disabled	2 CPs Assigned

Create Group:

Group Status

Click on a Group Name above to view or change.

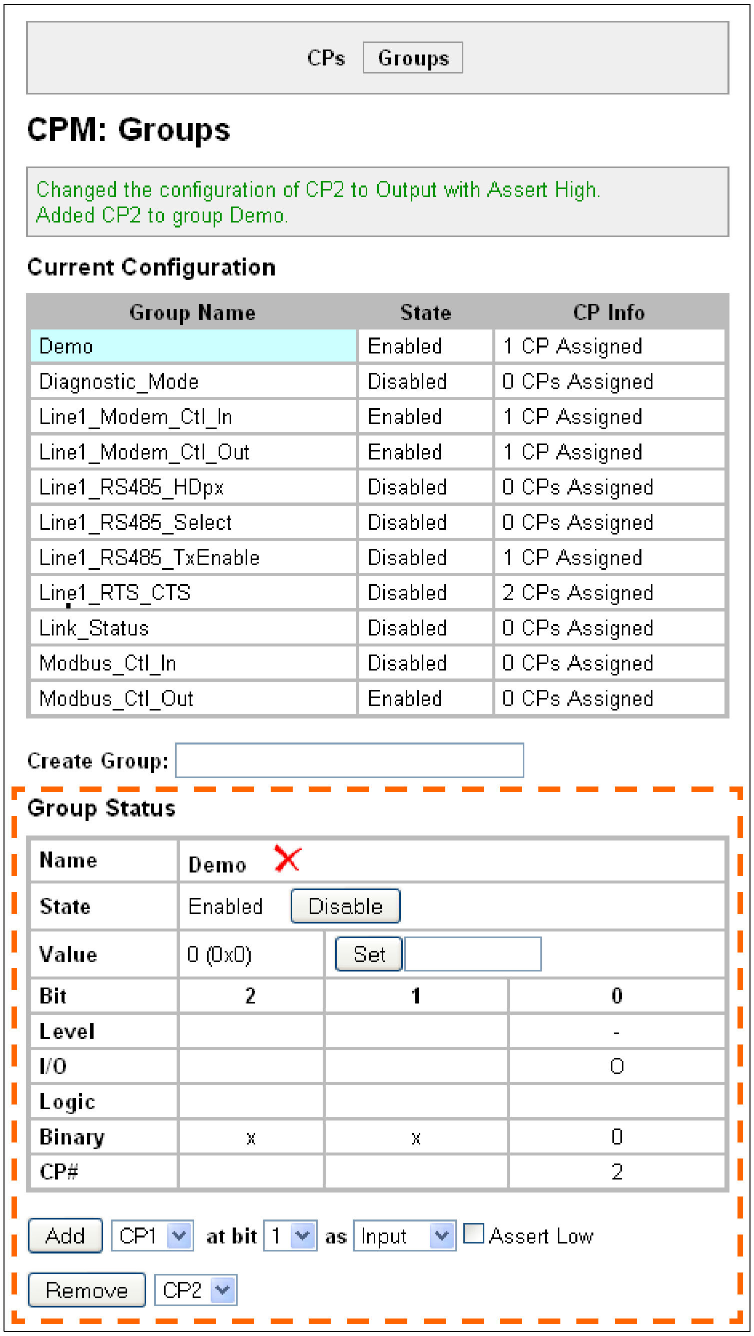
2. The Current Configuration table shows the current settings for each CP group.

Figure 8-5 CPM Groups Current Configuration

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

To display the status of a specific group:

1. Click **CPM > Groups**.
2. Click the CP group name in the Current Configuration table.



CPM: Groups

Changed the configuration of CP2 to Output with Assert High.
Added CP2 to group Demo.

Current Configuration

Group Name	State	CP Info
Demo	Enabled	1 CP Assigned
Diagnostic_Mode	Disabled	0 CPs Assigned
Line1_Modem_Ctl_In	Enabled	1 CP Assigned
Line1_Modem_Ctl_Out	Enabled	1 CP Assigned
Line1_RS485_HDpx	Disabled	0 CPs Assigned
Line1_RS485_Select	Disabled	0 CPs Assigned
Line1_RS485_TxEnable	Disabled	1 CP Assigned
Line1_RTS_CTS	Disabled	2 CPs Assigned
Link_Status	Disabled	0 CPs Assigned
Modbus_Ctl_In	Disabled	0 CPs Assigned
Modbus_Ctl_Out	Enabled	0 CPs Assigned

Create Group:

Group Status

Name	**Demo** ✕		
State	Enabled Disable		
Value	0 (0x0)	Set	
Bit	**2**	**1**	**0**
Level			-
I/O			O
Logic			
Binary	x	x	0
CP#			2

Add CP1 **at bit** 1 **as** Input □ Assert Low

Remove CP2

Figure 8-6 CPM: Group Status

Table 8-7 **Group Status**

CPM – Groups Page Group Status	Description
Name	Shows the CP Group name.
State	Shows the current state of the CP group. Locked groups are Lantronix default groups and cannot be deleted. Use the button in this field to enable or disable the group.
Value	Shows the CP group’s current value.

CPM – Groups Page Group Status	Description
Bit	Displays the individual bit positions for the available CPs.
Level	Indicates the voltage level of the CP. A plus sign (**+**) indicates the CP bit is asserted (the voltage is high). A minus sign (**-**) indicates the CP voltage is low.
I/O	Indicates the current status of the pin: ◆ **I** = input ◆ **O** = output ◆ **<blank>** = unassigned
Logic	Indicates the logic level of the CP. An "**I**" indicates the CP is inverted. A blank field indicates that the CP is not inverted.
Binary	Shows the assertion value of the corresponding bit. An **X** means that the group is disabled or the bit is unassigned in the group
CP#	Shows the configurable pin number and its bit position in the CP group.

To create a custom CP group:

1. Click **CPM > Groups**.
2. Enter a group name in the **Create Group** field.
3. Click **Submit**.

To add a CP to a Group

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

To delete a custom CP group:

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

To enable or disable a CP group:

1. Click **CPM > Groups**.
2. Select the Group name in the table representing the group you wish to enable. The Group Status information for this group appears in a table below.

3. Click **Enable** to enable, as appropriate.
4. Click **Disable** to disable, as appropriate.

To set a CP group's value:

1. Create a custom group and add a CP to it.
2. Click **CPM > Groups**.
3. Select the custom group from the current configuration table.
4. Enter a **Group Status Value**.
5. Click **Set**.

To remove a CP from a Group:

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

9: Service Settings

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

- *DNS Settings*
- *PPP Settings*
- *SNMP Settings*
- *FTP Settings*
- *TFTP Settings*
- *Syslog Settings*
- *HTTP Settings*
- *RSS Settings*

DNS Settings

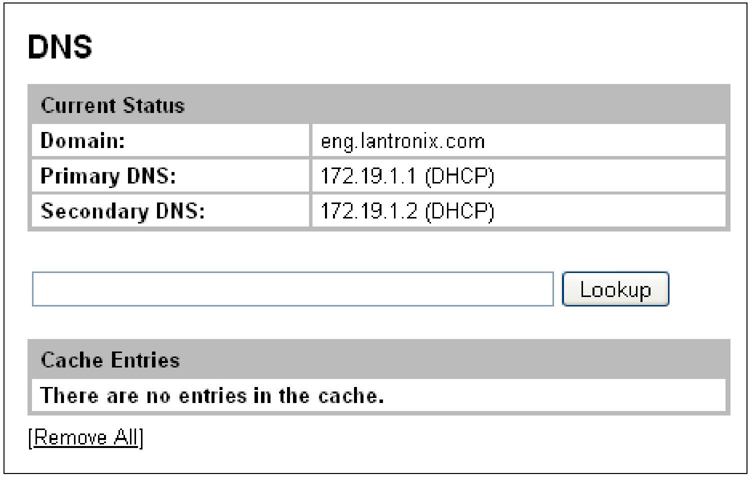
The primary and secondary domain name system (DNS) addresses come from the active interface. The static addresses from the Network Interface Configuration page may be overridden by DHCP or BOOTP. The DNS web page enables you to view the status and cache.

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

To view the DNS status:

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

Figure 9-1 DNS Settings



DNS

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

Cache Entries
There are no entries in the cache.

To find a DNS Name or IP Address:

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

To clear cache entries:

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

PPP Settings

Point-to-Point Protocol (PPP) establishes a direct connection between two nodes. It defines a method for data link connectivity between devices using physical layers (such as serial lines).

The XPort AR supports two types of PPP authentication: Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP). Both of these authentication methods require the configuration of a username and password.

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

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

Note: *RFC1334 defines both CHAP and PAP.*

The XPort AR also supports authentication scheme of "None" when no authentication is required during link negotiation.

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

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

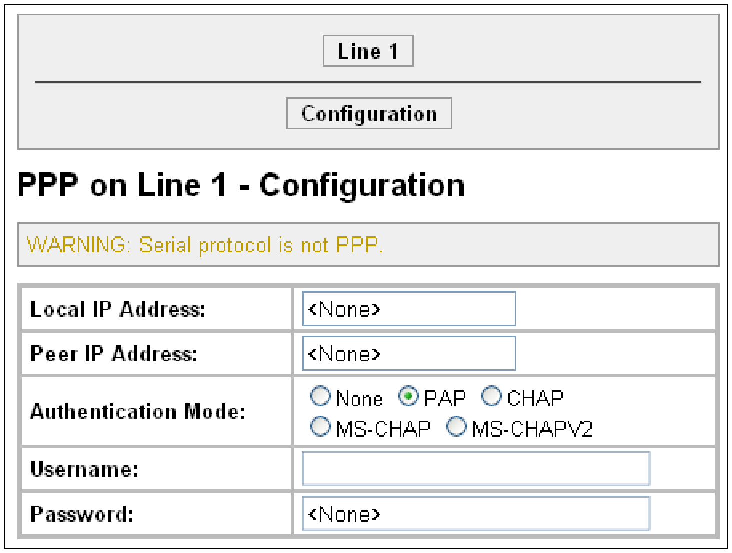
The XPort AR does not perform network address translation (NAT) between the serial-side network interface and the Ethernet/WLAN network interface. Therefore, to pass packets through the XPort AR, a static route must be configured on both the PPP Peer device and the remote device it wishes to communicate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

Note: *The following section describes the steps to configure PPP 1 (PPP on serial line 1); these steps also apply to any line instance of the device.*

To configure PPP:

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

Figure 9-2 PPP Configuration Settings



PPP on Line 1 - Configuration

WARNING: Serial protocol is not PPP.

Local IP Address:	<None>
Peer IP Address:	<None>
Authentication Mode:	○ None ● PAP ○ CHAP ○ MS-CHAP ○ MS-CHAPV2
Username:	
Password:	<None>

2. Enter or modify the following settings:

Table 9-3 **PPP Configuration**

PPP Configuration Settings	Description
Local IP Address	Enter the IP address assigned to the device's PPP interface.
Peer IP Address	Enter the IP address assigned to the peer (when requested during negotiation).
Authentication Mode	Choose the authentication mode: ◆ **None** = no authentication is required ◆ **PAP** = Password Authentication Protocol ◆ **CHAP** = Challenge Handshake Authentication Protocol ◆
Username	Enter a username if authentication is to be used on the PPP interface. The peer must be configured to use the same username.
Password	Enter a password if authentication is to be used on the PPP interface. The peer must be configured to use the same password.

3. Click **Submit.**

SNMP Settings

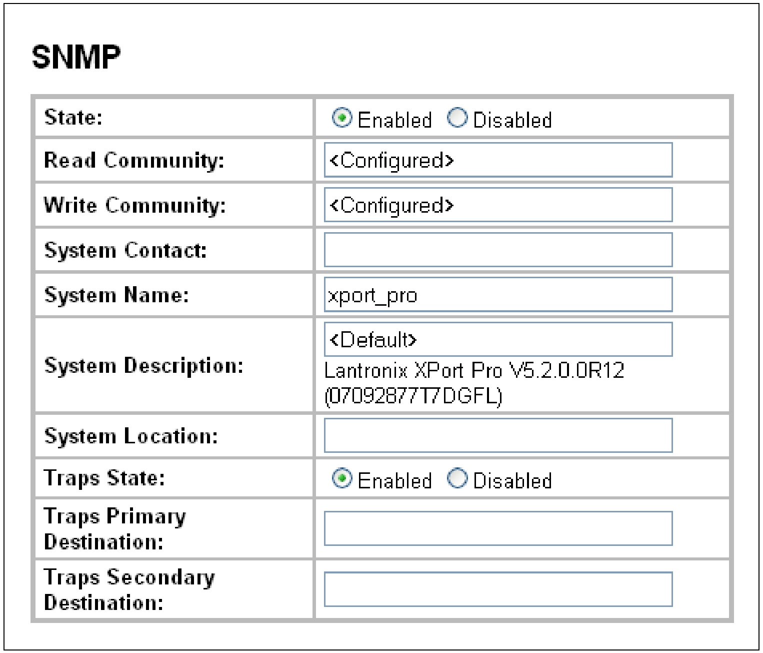
Simple Network Management Protocol (SNMP) is a network management tool that monitors network devices for conditions that need attention. The SNMP service responds to SNMP requests and generates SNMP Traps.

This page is used to configure the SNMP agent.

To configure SNMP:

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

Figure 9-4 SNMP Configuration



SNMP

State:	● Enabled ○ Disabled
Read Community:	<Configured>
Write Community:	<Configured>
System Contact:	
System Name:	xport_pro
System Description:	<Default> Lantronix XPort Pro V5.2.0.0R12 (0709287T7DGFL)
System Location:	
Traps State:	● Enabled ○ Disabled
Traps Primary Destination:	
Traps Secondary Destination:	

2. Enter or modify the following settings:

Table 9-5 **SNMP**

SNMP Settings	Description
State	Select **Enabled** 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.
Traps State	Select **Enabled** to enable the transmission of SNMP Traps. The Cold Start trap is sent on device boot up, and the Linkdown trap is sent when the device is rebooted from software control.
Traps Primary Destination	Enter the primary SNMP trap host.
Traps Secondary Destination	Enter the secondary SNMP trap host.

3. Click **Submit.**

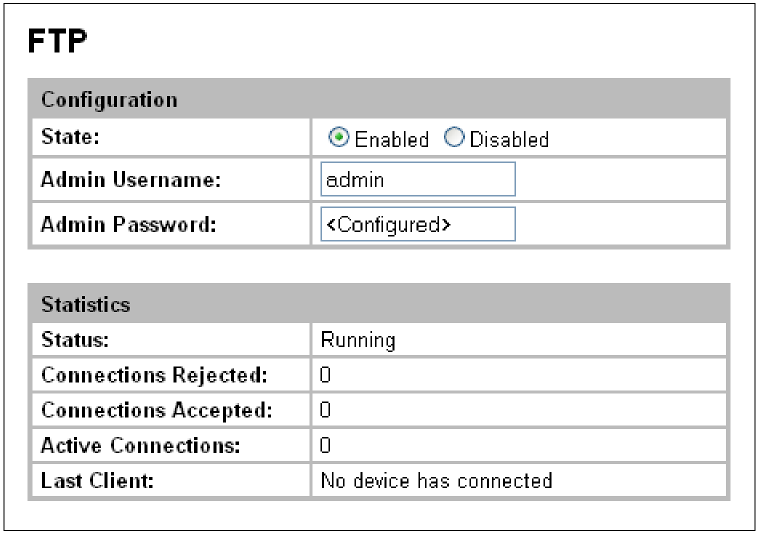
FTP Settings

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

To configure FTP:

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

Figure 9-6 FTP Configuration



FTP

Configuration	
State:	● Enabled ○ Disabled
Admin Username:	admin
Admin Password:	<Configured>

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

2. Enter or modify the following settings:

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

3. Click **Submit**.

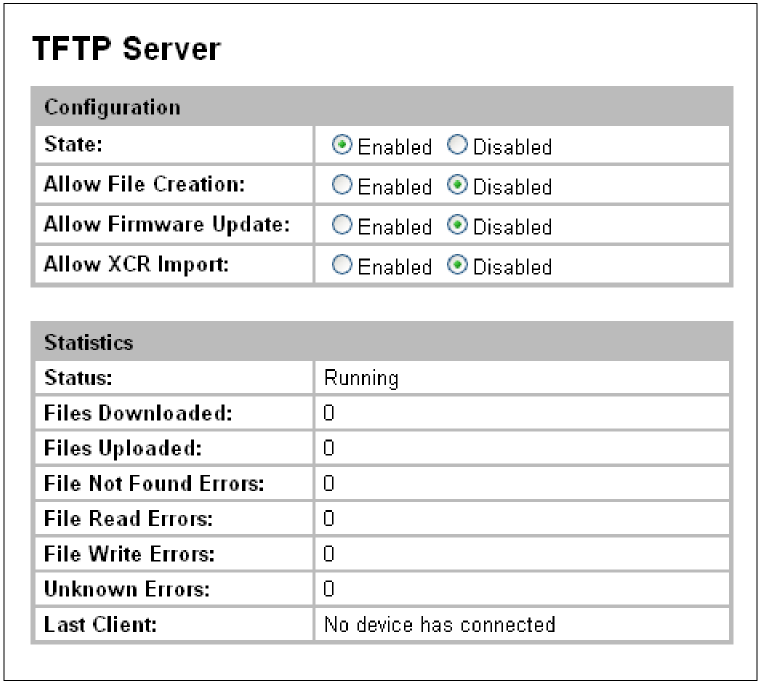
TFTP Settings

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

To configure TFTP:

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

Figure 9-7 TFTP Configuration



TFTP Server

Configuration	
State:	● Enabled ○ Disabled
Allow File Creation:	○ Enabled ● Disabled
Allow Firmware Update:	○ Enabled ● Disabled
Allow XCR Import:	○ Enabled ● Disabled

Statistics	
Status:	Running
Files Downloaded:	0
Files Uploaded:	0
File Not Found Errors:	0
File Read Errors:	0
File Write Errors:	0
Unknown Errors:	0
Last Client:	No device has connected

2. Enter or modify the following settings:

Table 9-8 **TFTP Server**

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

3. Click **Submit**.

Syslog Settings

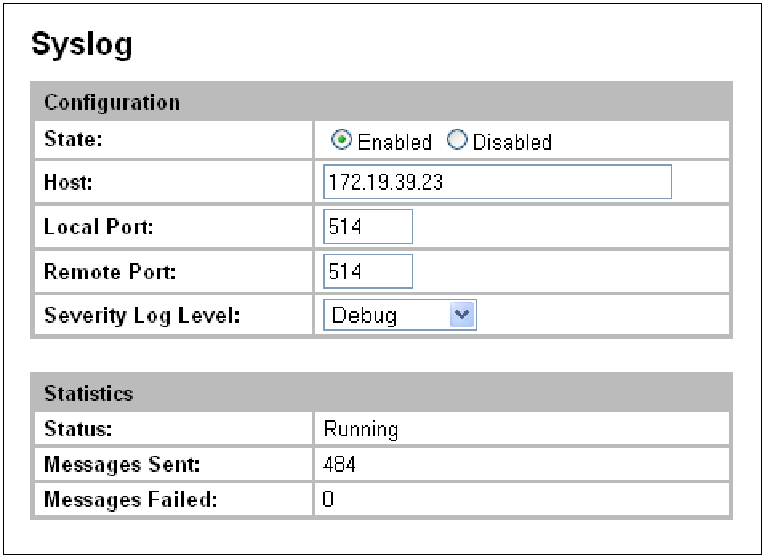
The Syslog web page shows the current configuration and statistics of the system log.

To configure the Syslog

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

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

Figure 9-9 Syslog



Syslog

Configuration	
State:	● Enabled ○ Disabled
Host:	172.19.39.23
Local Port:	514
Remote Port:	514
Severity Log Level:	Debug

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

2. Enter or modify the following settings:

Table 9-10 **Syslog**

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

3. Click **Submit**.

HTTP Settings

Hypertext Transfer Protocol (HTTP) is the transport protocol for communicating hypertext documents on the Internet. HTTP defines how messages are formatted and transmitted. It also defines the actions web servers and browsers should take in response to different commands. HTTP Authentication enables the requirement of usernames and passwords for access to the XPort AR device.

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

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

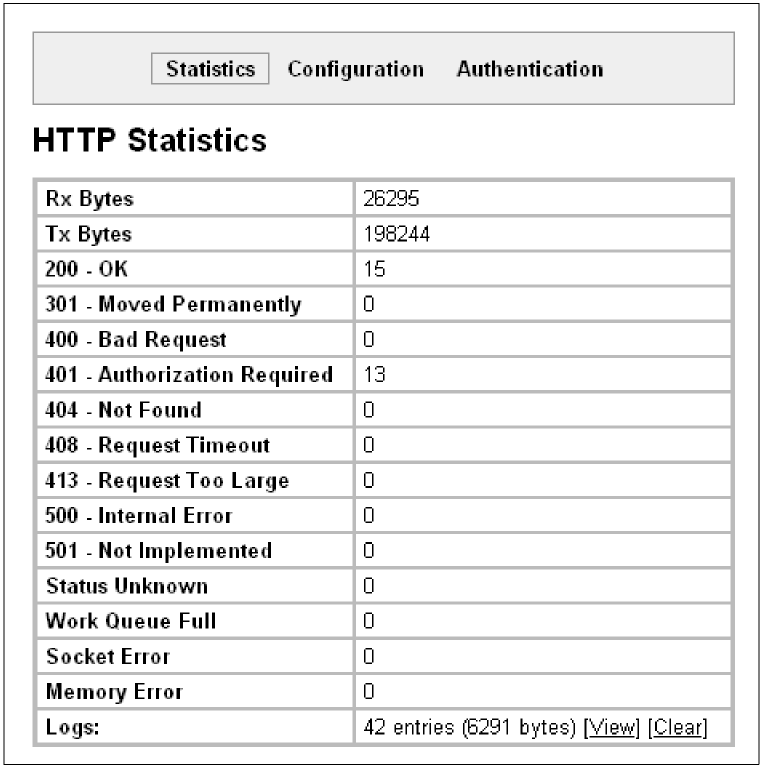
HTTP Statistics

To view HTTP statistics:

This page shows various statistics about the HTTP server.

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

Figure 9-11 HTTP Statistics



HTTP Statistics

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

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

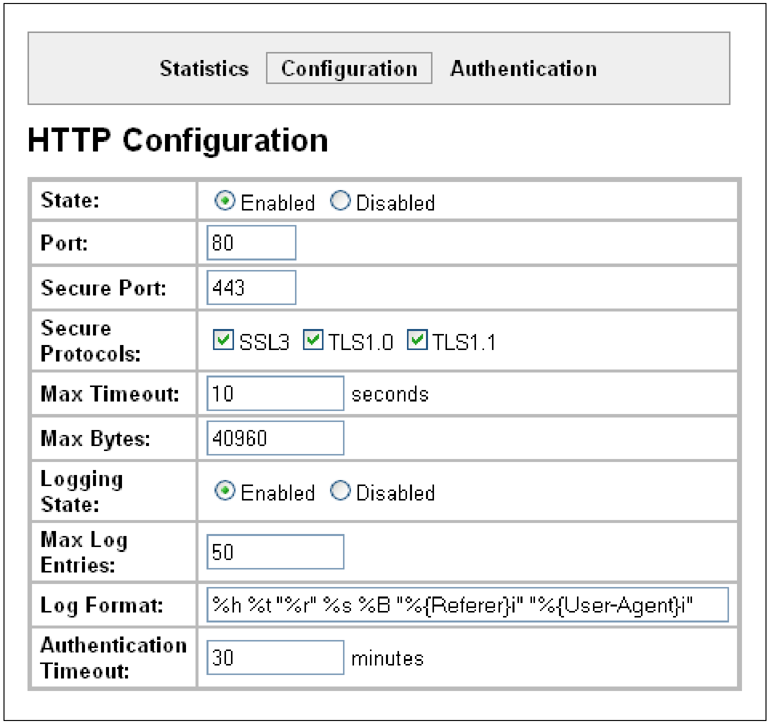
HTTP Configuration

On this page you may change HTTP configuration settings.

To configure HTTP:

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

Figure 9-12 HTTP Configuration



HTTP Configuration

State:	● Enabled ○ Disabled
Port:	80
Secure Port:	443
Secure Protocols:	☑ SSL3 ☑ TLS1.0 ☑ TLS1.1
Max Timeout:	10 seconds
Max Bytes:	40960
Logging State:	● Enabled ○ Disabled
Max Log Entries:	50
Log Format:	%h %t "%r" %s %B "%{Referer}i" "%{User-Agent}i"
Authentication Timeout:	30 minutes

2. Enter or modify the following settings:

Table 9-13 **HTTP Configuration**

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

HTTP Configuration Settings (continued)	Description
Secure Protocols	Select to enable or disable the following protocols: ◆ **SSL3** = Secure Sockets Layer version 3 ◆ **TLS1.0** = Transport Layer Security version 1.0. TLS 1.0 is the successor of SSL3 as defined by the IETF. ◆ **TLS1.1** = Transport Layer Security version 1.1 The protocols are enabled by default. *Note: A server certificate and associated private key need to be installed in the* **SSL** *configuration section to use* **HTTPS***.*
Max Timeout	Enter the maximum time for the HTTP server to wait when receiving a request. This prevents Denial-of-Service (DoS) attacks. The default is **10** seconds.
Max Bytes	Enter the maximum number of bytes the HTTP server accepts when receiving a request. The default is **40** kB (this prevents DoS attacks).
Logging State	Select **Enabled** to enable HTTP server logging.
Max Log Entries	Sets the maximum number of HTTP server log entries. Only the last **Max Log Entries** are cached and viewable.
Log Format	Set the log format string for the HTTP server. Follow these **Log Format** rules: ◆ **%a** - remote IP address (could be a proxy) ◆ **%b** - bytes sent excluding headers ◆ **%B** - bytes sent excluding headers (0 = '-') ◆ **%h** - remote host (same as '%a') ◆ **%{h}i** - header contents from request (h = header string) ◆ **%m** - request method ◆ **%p** - ephemeral local port value used for request ◆ **%q** - query string (prepend with '?' or empty '-') ◆ **%t** - timestamp HH:MM:SS (same as Apache '%(%H:%M:%S)t' or '%(%T)t') ◆ **%u** - remote user (could be bogus for 401 status) ◆ **%U** - URL path info ◆ **%r** - first line of request (same as '%m %U%q <version>') ◆ **%s** - return status
Authentication Timeout	The timeout period applies if the selected authentication type is either **Digest** or **SSL/Digest**. After this period of inactivity, the client must authenticate again.

3. Click **Submit.**

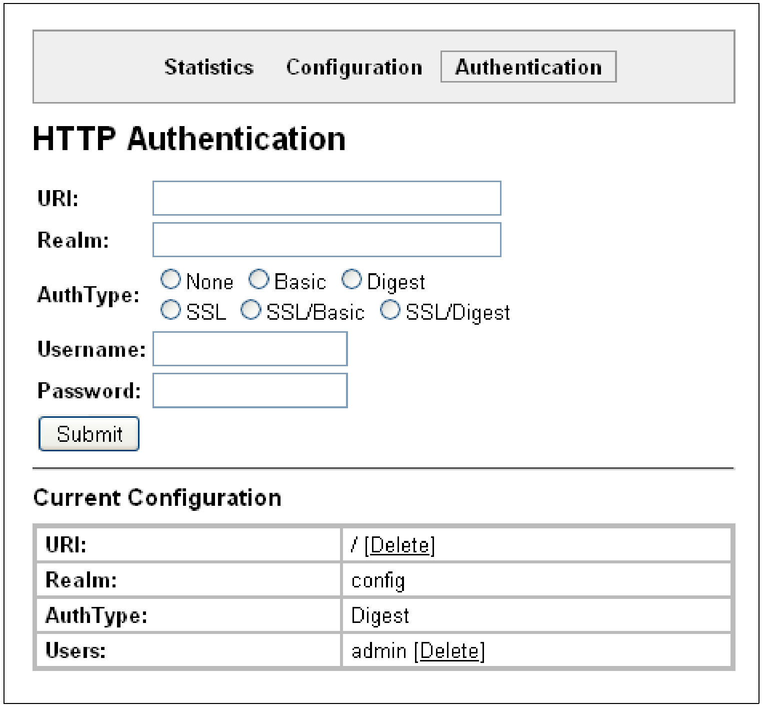
HTTP Authentication

HTTP Authentication enables you to require usernames and passwords to access specific web pages or directories on the XPort 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 9-14 HTTP Authentication



HTTP Authentication

URI:

Realm:

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

Username:

Password:

Current Configuration

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

2. Enter or modify the following settings:

Table 9-15 **HTTP Authentication**

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

HTTP Authentication Settings (continued)	Description
Auth Type	Select the authentication type: ◆ **None** = no authentication is necessary. ◆ **Basic** = encodes passwords using Base64. ◆ **Digest** = encodes passwords using MD5. ◆ **SSL** = the page can only be accessed over SSL (no password is required). ◆ **SSL/Basic** = the page is accessible only over SSL and encodes passwords using Base64. ◆ **SSL/Digest** = the page is accessible only over SSL and encodes passwords using MD5. *Note: When changing the parameters of Digest or SSL Digest authentication, it is often best to close and reopen the browser to ensure it does not attempt to use cached authentication information.*
Username	Enter the **Username** used to access the **URI**. More than one Username per URI is permitted. Click **Submit** and enter the next Username as necessary.
Password	Enter the **Password** for the **Username**.

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

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

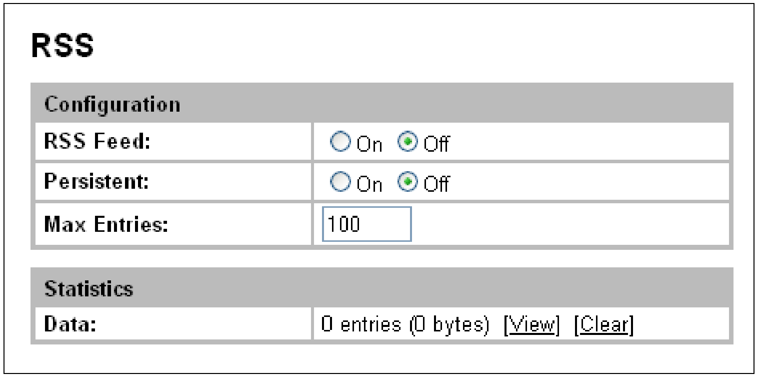
RSS Settings

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

To configure RSS settings:

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

Figure 9-16 RSS



RSS

Configuration	
RSS Feed:	○ On ● Off
Persistent:	○ On ● Off
Max Entries:	100

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

2. Enter or modify the following settings:

***Table 9-17* RSS**

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

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

10: Security Settings

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

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

Note: *The XPort AR supports SSLv3 and its successors, TLS1.0 and TLS1.1. An incoming SSlv2 connection attempt is answered with an SSlv3 response. If the initiator also supports SSLv3, SSLv3 handles the rest of the connection.*

This chapter contains the following sections:

SSH Settings

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

Two instances require configuration: when the XPort 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. The SSH client is for tunneling in Connect Mode.

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

- **Defined host keys:** both private and public keys are required. These keys are used for the Diffie-Hellman key exchange (used for the underlying encryption protocol).
- **Defined users:** these users are permitted to connect to the XPort AR SSH server.

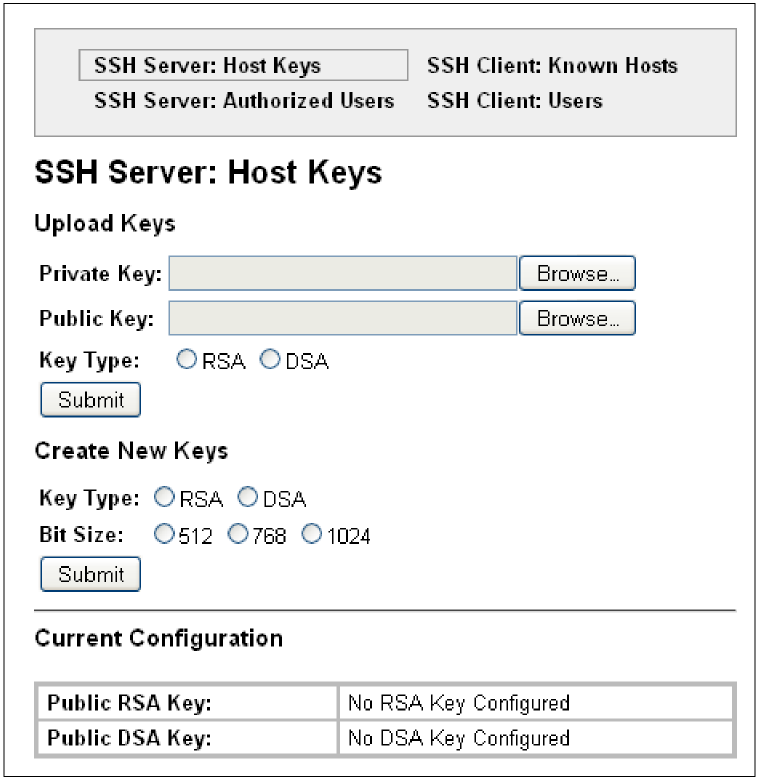
This page has four links at the top for viewing and changing SSH server host keys, SSH server authorized keys, SSH client known hosts, and SSH client users.

SSH Server Host Keys

To configure the SSH server host keys:

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

Figure 10-1 SSH Server: Host Keys



SSH Server: Host Keys

Upload Keys

Private Key: [ ] Browse...

Public Key: [ ] Browse...

Key Type: ○ RSA ○ DSA

Submit

Create New Keys

Key Type: ○ RSA ○ DSA

Bit Size: ○ 512 ○ 768 ○ 1024

Submit

Current Configuration

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

2. Enter or modify the following settings:

***Table 10-2* SSH Server Host Keys Settings**

SSH Server: Host Keys 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. *Note: RSA is more secure.*

SSH Server: Host Keys Settings (continued)	Description
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 Using a larger bit size takes more time to generate the key. Approximate times are: ◆ 2 minutes for a 512 bit RSA Key ◆ 5 minutes for a 768 bit RSA Key ◆ 15 minutes for a 1024 bit RSA Key ◆ 10 minutes for a 512 bit DSA Key ◆ 30 minutes for a 768 bit DSA Key ◆ 70 minutes for a 1024 bit DSA key *Note: Some SSH clients require RSA host keys to be at least 1024 bits long. This device generates keys up to 1024 bits long. It can work with larger keys (up to 2048 bit) if they are imported or otherwise created.*

3. Click **Submit.**

Note: SSH keys may be created on another computer and uploaded to the XPort AR. For example, use the following command using Open SSH to create a 1024-bit DSA key pair: `ssh-keygen –b 1024 –t dsa`

SSH Keys from other programs may be converted to the required XPort AR format. Use Open SSH to perform the conversion.

To convert from RFC-4716 format: `ssh-keygen –i`

For more options, look at the help from Open SSH: `ssh-keygen ?`

1. 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 longer key generation times.

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

Note: When uploading the security keys, ensure the keys are not compromised in transit.

SSH Server Authorized Users

On this page you can change SSH server settings for Authorized Users. SSH Server Authorized Users are accounts on the XPort AR that can be used to log into the XPort 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.

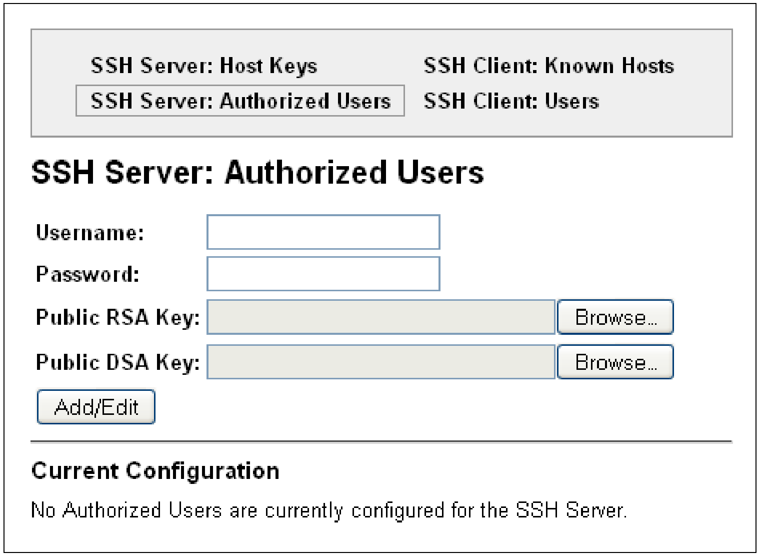
The user's public keys are optional and only necessary if public key authentication is required. Using public key authentication allows a connection to be made without the password being asked.

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 appears.

Figure 10-3 SSH Server: Authorized Users



SSH Server: Authorized Users

Current Configuration

No Authorized Users are currently configured for the SSH Server.

2. Enter or modify the following settings:

***Table 10-4* SSH Server Authorized User Settings**

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

3. Click **Submit.**

SSH Client Known Hosts

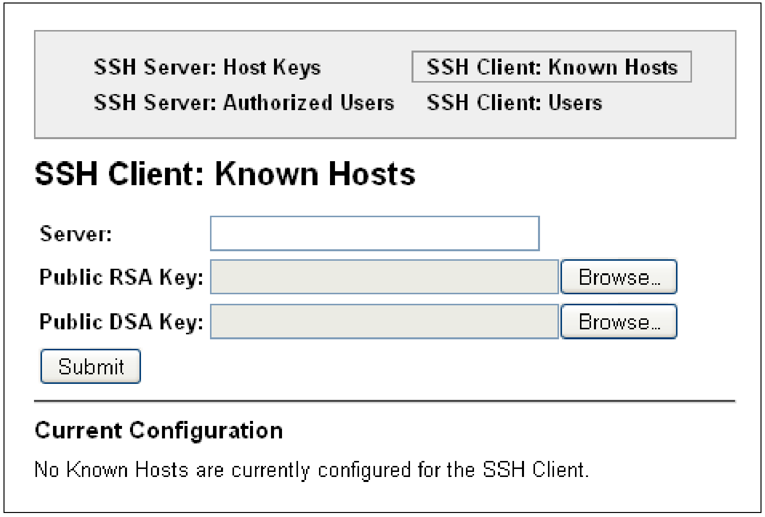
On this page you can change SSH client settings for known hosts.

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 appears.

Figure 10-5 SSH Client: Known Hosts



No Known Hosts are currently configured for the SSH Client.

2. Enter or modify the following settings:

Table 10-6 **SSH Client Known Hosts**

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

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

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

SSH Client User

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

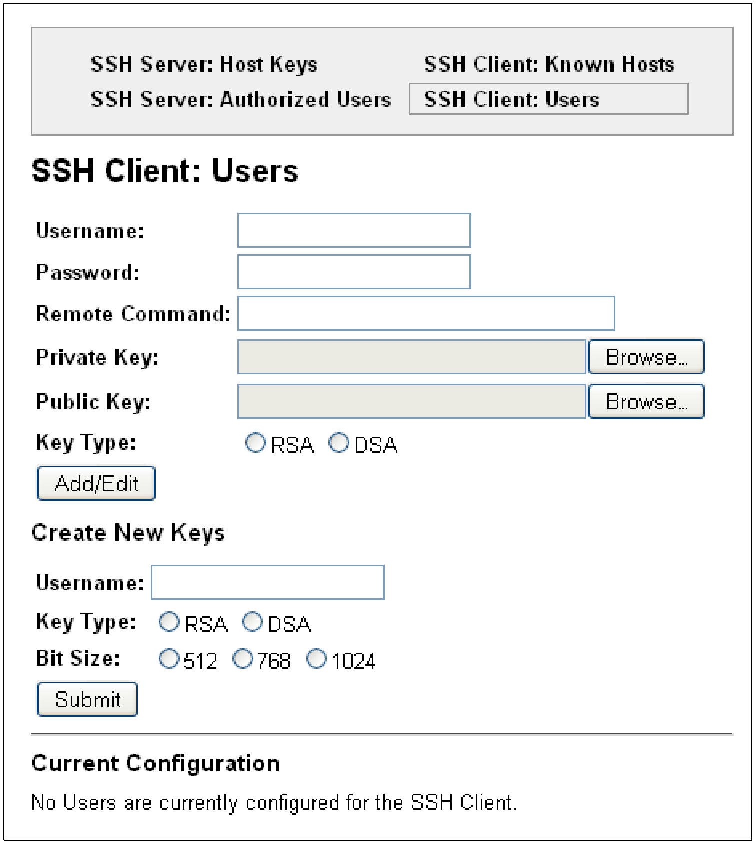
SSH client known users are used by all applications that play the role of an SSH client, specifically tunneling in Connect Mode. At the very least, a password or key pair must be configured for a user. The keys for public key authentication can be created elsewhere and uploaded to the device or automatically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

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

To configure the SSH client users:

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

Figure 10-7 SSH Client: Users



No Users are currently configured for the SSH Client.

2. Enter or modify the following settings:

Table 10-8 **SSH Client Users**

SSH Client: Users Settings	Description
Username	Enter the name that the device uses to connect to a SSH server.
Password	Enter the password associated with the username.
Remote Command	Enter the command that can be executed remotely. Default is **shell**, which tells the SSH server to execute a remote shell upon connection. This command can be changed to anything the remote host can perform.
Private Key	Enter the name of the existing private key you want to use with this SSH client user. You can either enter the path and name of the key, or use the **Browse** button to select the key.
Public Key	Enter the path and name of the existing public key you want to use with this SSH client user or use the **Browse** button to select the key. *Note: If the user public key is known on the remote SSH server, the SSH server does not require a password. The* **Remote Command** *is provided to the SSH server upon connection. It specifies the application to execute upon connection. The default is a command shell.* *Note: Configuring the SSH client's known hosts is optional. It prevents Man-In-The-Middle (MITM) attacks*
Key Type	Select the key type to be used. Choices are: ◆ **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: ◆ 2 minutes for a 512 bit RSA Key ◆ 5 minutes for a 768 bit RSA Key ◆ 15 minutes for a 1024 bit RSA Key ◆ 10 minutes for a 512 bit DSA Key ◆ 30 minutes for a 768 bit DSA Key ◆ 70 minutes for a 1024 bit DSA key *Note: Some SSH clients require RSA host keys to be at least 1024 bits long. This device generates keys up to 1024 bits long. It can work with larger keys (up to 2048 bit) if they are imported or otherwise created.*

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

SSL Settings

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

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

For more information regarding Certificates and how to obtain them, see *SSL Certificates and Private Keys (on page 83).*

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

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

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

The XPort AR supports SSlv3 and its successors, TLS1.0 and TLS1.1.

Note: *An incoming SSlv2 connection attempt is answered with an SSlv3 response. If the initiator also supports SSLv3, SSLv3 handles the rest of the connection.*

SSL Cipher Suites

The SSL standard defines only certain combinations of certificate type, key exchange method, symmetric encryption, and hash method. Such a combination is called a cipher suite. Supported cipher suites include the following:

Table 10-9 **Supported Cipher Suites**

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

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

SSL Certificates

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

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

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

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

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

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

SSL RSA or DSA

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

SSL Certificates and Private Keys

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

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

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

SSL Utilities

Several utilities exist to convert between the formats.

OpenSSL

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

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

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

Steel Belted Radius

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

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

The sbr_certkey.pem file contains both certificate and key. If loading the SBR certificate into XPort AR as an authority, you will need to edit it.

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

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

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

FreeRadius

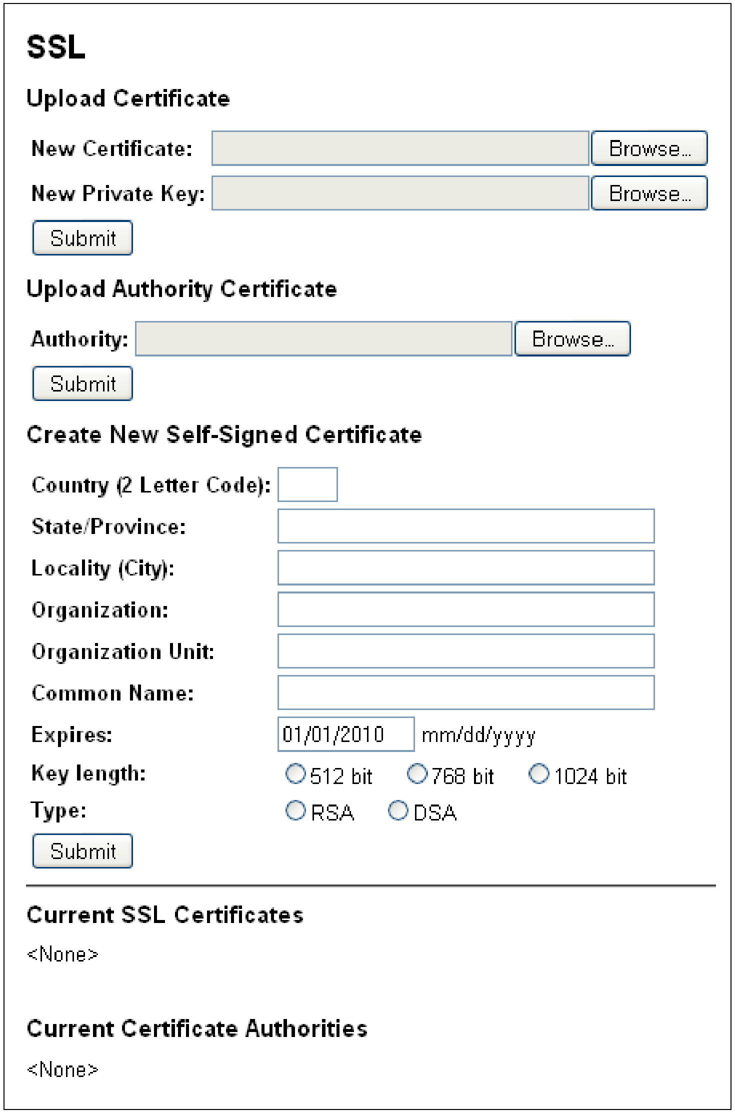
Free Radius is a Linux open-source Radius server. It is versatile, but complicated to configure.

SSL Configuration

To configure SSL settings:

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

Figure 10-10 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

Key length: ○ 512 bit ○ 768 bit ○ 1024 bit

Type: ○ RSA ○ DSA

Submit

Current SSL Certificates

<None>

Current Certificate Authorities

<None>

2. Enter or modify the following settings:

Table 10-11 **SSL**

SSL Settings	Description
Upload Certificate	
New Certificate	This certificate identifies the device to peers. It is used for HTTPS and SSL Tunneling. Enter the path and name of the certificate you want to upload, or use the **Browse** button to select the certificate. **RSA** or **DSA** certificates with 512 to 1024 bit public keys are allowed. The format of the file must be **PEM**. The file must start with “-----BEGIN CERTIFICATE-----“ and end with “-----END CERTIFICATE-----“. Some Certificate Authorities add comments before and/or after these lines. Those need to be deleted before upload.
New Private Key	Enter the path and name of the private key you want to upload, or use the **Browse** button to select the private key. The key needs to belong to the certificate entered above. The format of the file must be **PEM**. The file must start with “-----BEGIN RSA PRIVATE KEY-----” and end with “-----END RSA PRIVATE KEY-----”. Read **DSA** instead of **RSA** in case of a **DSA** key. Some Certificate Authorities add comments before and/or after these lines. Those need to be deleted before upload.
Upload Authority Certificate	
Authority	One or more authority certificates are needed to verify a peer's identity. It is used for SSL Tunneling. These certificates do not require a private key. Enter the path and name of the certificate you want to upload, or use the **Browse** button to select the certificate. **RSA** or **DSA** certificates with 512 to 1024 bit public keys are allowed. The format of the file must be **PEM**. The file must start with “-----BEGIN CERTIFICATE-----” and end with “-----END CERTIFICATE-----”. Some Certificate Authorities add comments before and/or after these lines. Those need to be deleted before upload.
Create New Self-Signed Certificate	
Country (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.

SSL Settings (continued)	Description
Common Name	Enter the same name that the user will enter when requesting your web site. **Example:** If a user enters http://www.widgets.abccompany.com to access your web site, the **Common Name** would be www.widgets.abccompany.com.
Expires	Enter the expiration date, in mm/dd/yyyy format, for the new self-signed certificate. **Example:** An expiration date of May 9, 2010 is entered as 05/09/2010.
Key length	Select the bit size of the new self-signed certificate. Choices are: ◆ **512 bits** ◆ **768 bits** ◆ **1024 bits** The larger the bit size, the longer it takes to generate the key. Approximate times are: ◆ 2 minutes for a 512 bit RSA Key ◆ 5 minutes for a 768 bit RSA Key ◆ 15 minutes for a 1024 bit RSA Key ◆ 10 minutes for a 512 bit DSA Key ◆ 30 minutes for a 768 bit DSA Key ◆ 70 minutes for a 1024 bit DSA key ◆
Type	Select the type of key: ◆ **RSA** = Public-Key Cryptography algorithm based on large prime numbers, invented by Rivest Shamir and Adleman. Used for encryption and signing. ◆ **DSA** = Digital Signature Algorithm also based on large prime numbers, but can only be used for signing. Developed by the US government to avoid the patents on RSA.

3. Click **Submit**.

11: Maintenance and Diagnostics Settings

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

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

Filesystem Settings

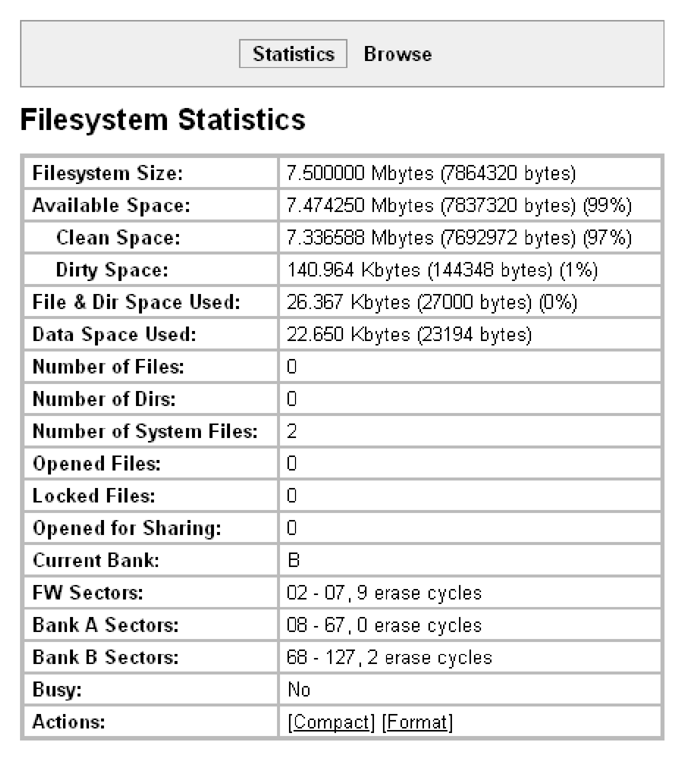
The XPort AR uses a flash filesystem to store files. Use the Filesystem option to view current file statistics or modify files. There are two subsections: Statistics and Browse.

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

Filesystem Statistics

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

Figure 11-1 Filesystem Statistics



Filesystem Statistics

Filesystem Size:	7.500000 Mbytes (7864320 bytes)
Available Space:	7.474250 Mbytes (7837320 bytes) (99%)
Clean Space:	7.336588 Mbytes (7692972 bytes) (97%)
Dirty Space:	140.964 Kbytes (144348 bytes) (1%)
File & Dir Space Used:	26.367 Kbytes (27000 bytes) (0%)
Data Space Used:	22.650 Kbytes (23194 bytes)
Number of Files:	0
Number of Dirs:	0
Number of System Files:	2
Opened Files:	0
Locked Files:	0
Opened for Sharing:	0
Current Bank:	B
FW Sectors:	02 - 07, 9 erase cycles
Bank A Sectors:	08 - 67, 0 erase cycles
Bank B Sectors:	68 - 127, 2 erase cycles
Busy:	No
Actions:	[Compact] [Format]

To view filesystem statistics or to compact or format the filesystem:

1. Back up all files as necessary.
2. Click **Filesystem** on the menu bar. The Filesystem page opens and shows the current filesystem statistics and usage.
3. To compact the files, click **Compact** in the Actions row.

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

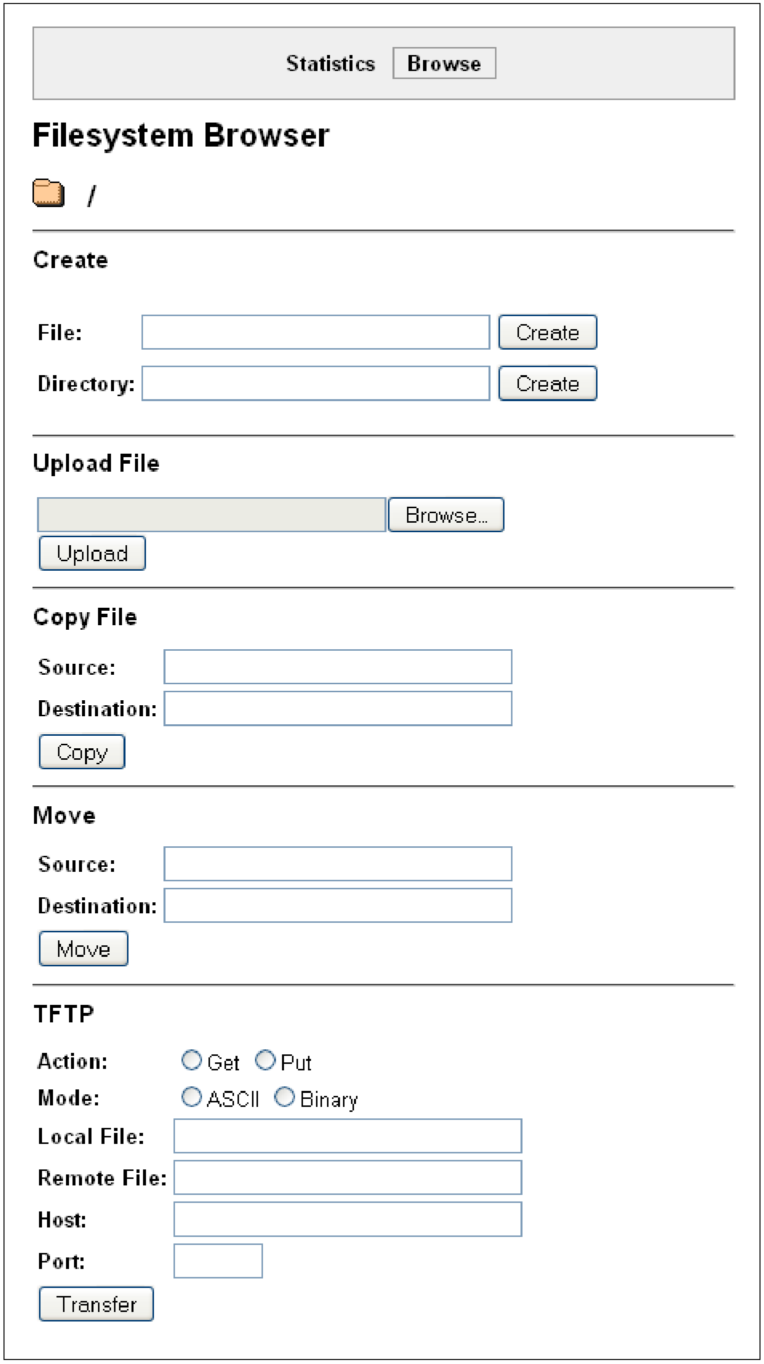
4. Back up all files before you perform the next (Format) step, because all user files get erased in that step.
5. Click **Format** in the Actions row. The configuration gets retained.

Filesystem Browser

To browse the filesystem:

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

Figure 11-2 Filesystem Browser



Statistics | Browse

Filesystem Browser

/

Create

File: [ ] Create

Directory: [ ] Create

Upload File

[ ] Browse...

Upload

Copy File

Source: [ ]

Destination: [ ]

Copy

Move

Source: [ ]

Destination: [ ]

Move

TFTP

Action: ○ Get ○ Put

Mode: ○ ASCII ○ Binary

Local File: [ ]

Remote File: [ ]

Host: [ ]

Port: [ ]

Transfer

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.

Table 11-3 **Filesystem Browser**

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

Protocol Stack Settings

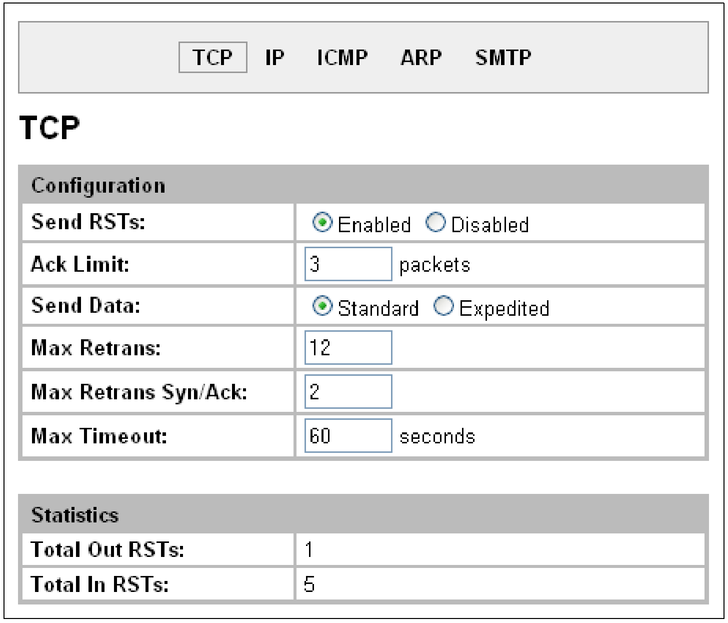
In the Protocol Stack web page, you can configure TCP, IP, ICMP, SMTP and ARP.

TCP Settings

To configure the TCP network protocol:

1. Click **Protocol Stack** on the menu bar.
2. Click **TCP**.

Figure 11-4 TCP Protocol



TCP

Configuration	
Send RSTs:	● Enabled ○ Disabled
Ack Limit:	3 packets
Send Data:	● Standard ○ Expedited
Max Retrans:	12
Max Retrans Syn/Ack:	2
Max Timeout:	60 seconds

Statistics	
Total Out RSTs:	1
Total In RSTs:	5

3. Modify the following settings:

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

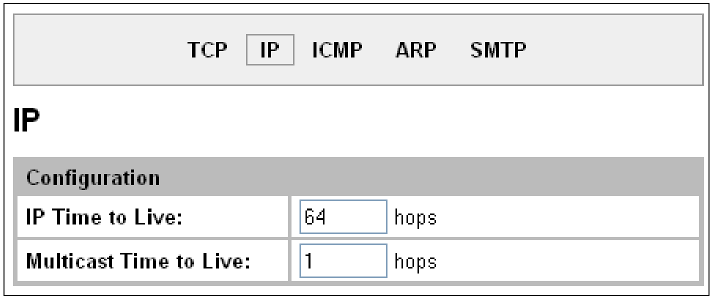
Protocol Stack TCP Settings	Description
Max Retrans Syn/Ack	Enter the maximum number of retransmissions of a SYN that will be attempted before failing. It is lower than “Max Retrans” to thwart denial-of-service attacks.
Max Timeout	Enter the maximum time between retransmissions.

4. Click **Submit**.

IP Settings

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

Figure 11-5 IP Protocol



IP Time to Live: 64 hops

Multicast Time to Live: 1 hops

3. Modify the following settings:

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

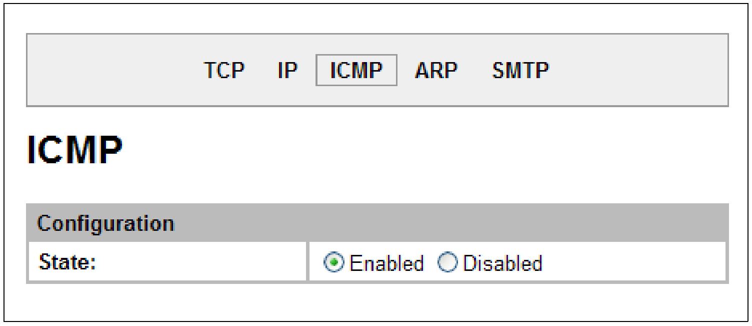
4. Click **Submit**.

ICMP Settings

To configure the ICMP network protocol:

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

Figure 11-6 ICMP Protocol



ICMP

Configuration

State: ● Enabled ○ Disabled

3. Select the appropriate state.

Table 11-7 **ICMP Settings**

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

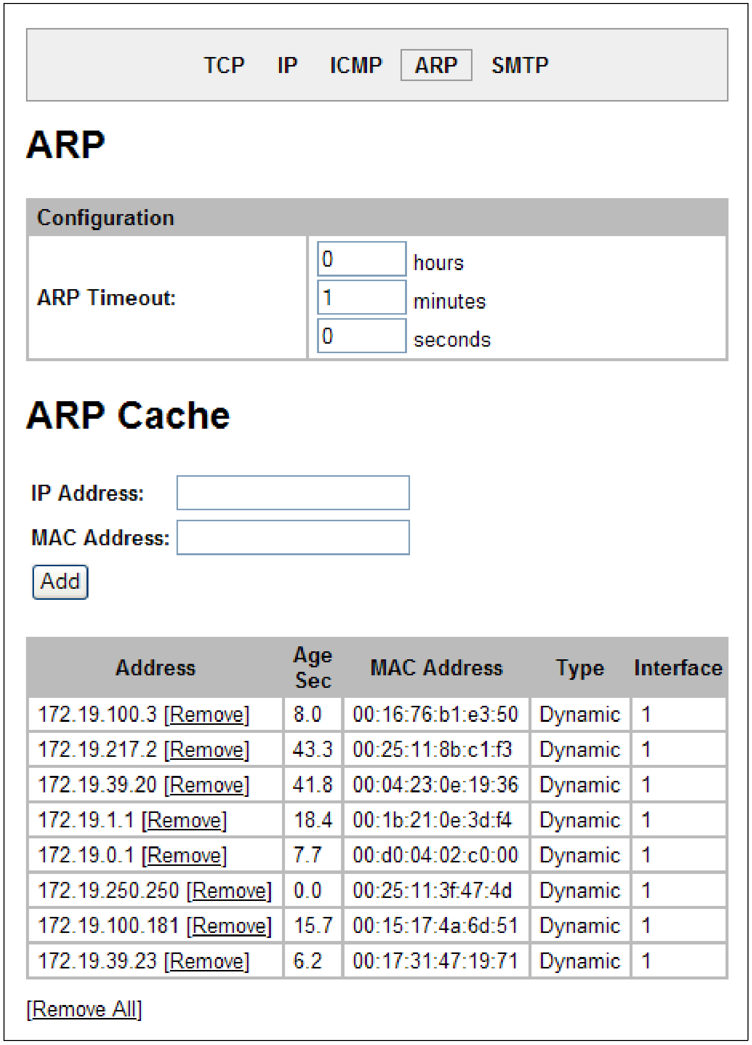
4. Click **Submit**.

ARP Settings

To configure the ARP network protocol:

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

Figure 11-8 ARP Protocol Page



ARP

Configuration

ARP Timeout: 0 hours 1 minutes 0 seconds

ARP Cache

IP Address:

MAC Address:

Address	Age Sec	MAC Address	Type	Interface
172.19.100.3 [Remove]	8.0	00:16:76:b1:e3:50	Dynamic	1
172.19.217.2 [Remove]	43.3	00:25:11:8b:c1:f3	Dynamic	1
172.19.39.20 [Remove]	41.8	00:04:23:0e:19:36	Dynamic	1
172.19.1.1 [Remove]	18.4	00:1b:21:0e:3d:f4	Dynamic	1
172.19.0.1 [Remove]	7.7	00:d0:04:02:c0:00	Dynamic	1
172.19.250.250 [Remove]	0.0	00:25:11:3f:47:4d	Dynamic	1
172.19.100.181 [Remove]	15.7	00:15:17:4a:6d:51	Dynamic	1
172.19.39.23 [Remove]	6.2	00:17:31:47:19:71	Dynamic	1

[Remove All]

3. Modify the following settings:

***Table 11-9* ARP Settings**

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

Table 11-9 **ARP Settings**

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

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

4. Click **Submit** for ARP or **Add** after supplying both address fields for ARP cache.
5. Remove entries from the ARP cache, as desired:
   - Click **Remove All** to remove all entries in the ARP cache.

     OR
   - Click **Remove** beside a specific entry to remove it from the ARP cache.

SMTP Settings

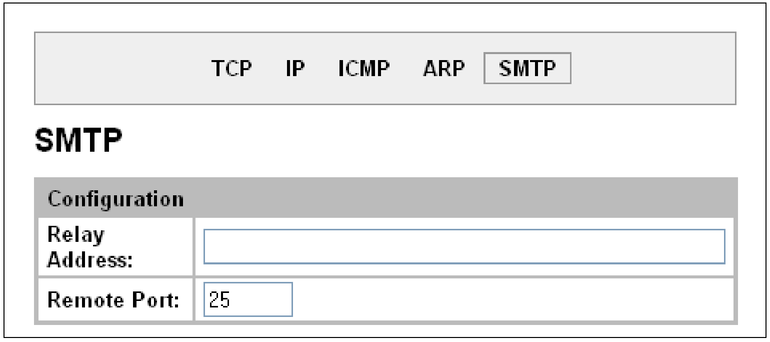
SMTP is configuration for a basic SMTP proxy. An SMTP proxy in this sense is a simple forwarding agent.

Note: *Lantronix does not support SMTP AUTH or any other authentication or encryption schemes for email. Please see Email Settings on page 111 for additional information.*

To configure the SMTP network protocol:

1. Click **Protocol Stack** on the menu bar.
2. Click **SMTP**.

Figure 11-10 SMTP



SMTP

Configuration

Relay Address:

Remote Port: 25

3. Modify the following settings:

Table 11-11 **SMTP Settings**

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

4. Click **Submit**.

IP Address Filter

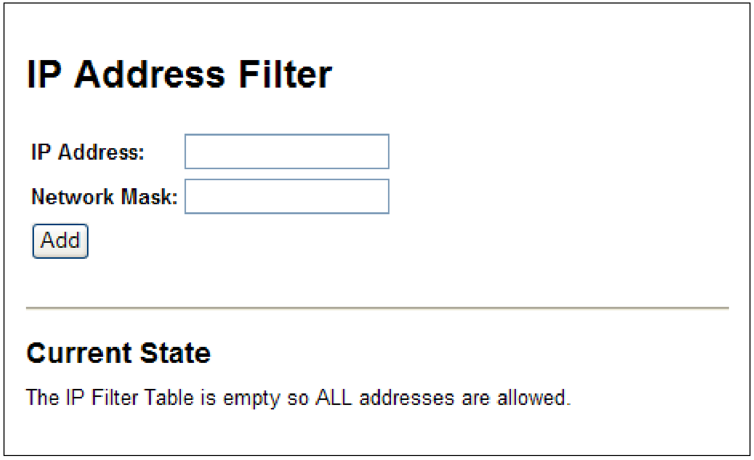
The IP address filter specifies the hosts and subnets permitted to communicate with the XPort AR device.

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 11-12 IP Address Filter Configuration



IP Address Filter

IP Address:

Network Mask:

Current State

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

Note: *If you enter any filter, be careful to make sure that your network IP address is covered. Otherwise you will loose access to the XPort AR. You will have to then access the XPort AR from a different computer to reset the configuration.*

2. Enter or modify the following settings:

Table 11-13 **IP Address Filter Settings**

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

3. Click **Add.**

Note: *In the Current State table, click* **Remove** *to delete any existing settings, as necessary.*

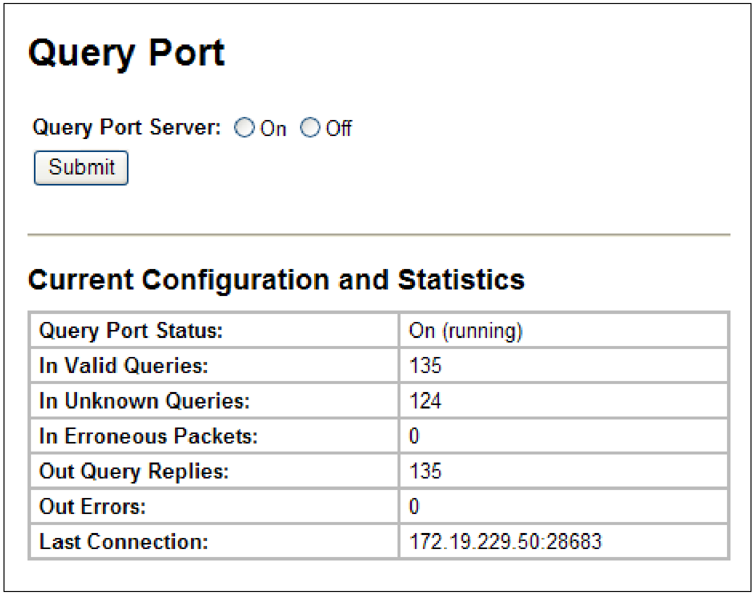
Query Port

The query port (0x77FE) is used for the automatic discovery of the device by the DeviceInstaller utility. Only 0x77FE discover messages from DeviceInstaller are supported. For more information on DeviceInstaller, see *Using DeviceInstaller (on page 19)*.

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 11-14 Query Port Configuration



Query Port

Query Port Server: ○ On ○ Off

Current Configuration and Statistics

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

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

Diagnostics

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

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

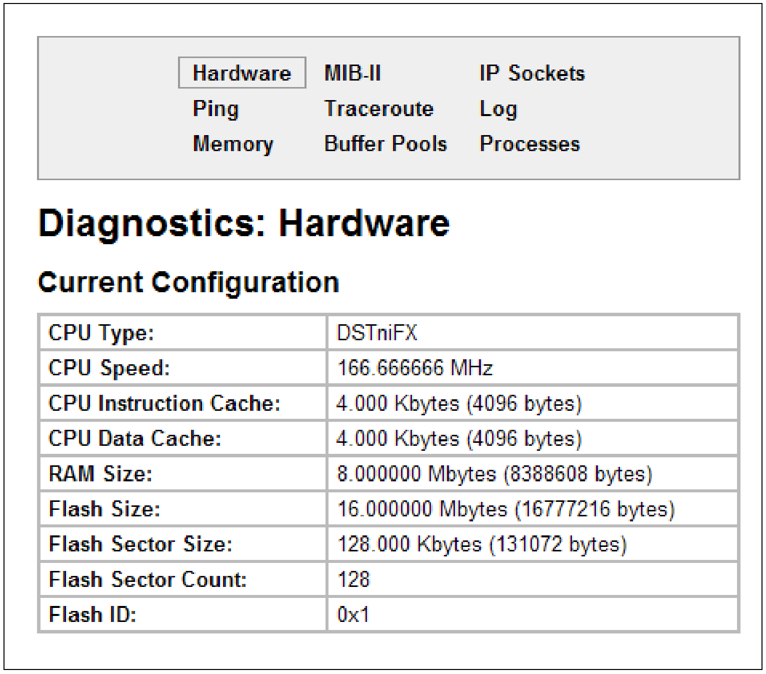
Hardware

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

To display hardware diagnostics:

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

Figure 11-15 Diagnostics: Hardware



Diagnostics: Hardware

Current Configuration

CPU Type:	DSTniFX
CPU Speed:	166.666666 MHz
CPU Instruction Cache:	4.000 Kbytes (4096 bytes)
CPU Data Cache:	4.000 Kbytes (4096 bytes)
RAM Size:	8.000000 Mbytes (8388608 bytes)
Flash Size:	16.000000 Mbytes (16777216 bytes)
Flash Sector Size:	128.000 Kbytes (131072 bytes)
Flash Sector Count:	128
Flash ID:	0x1

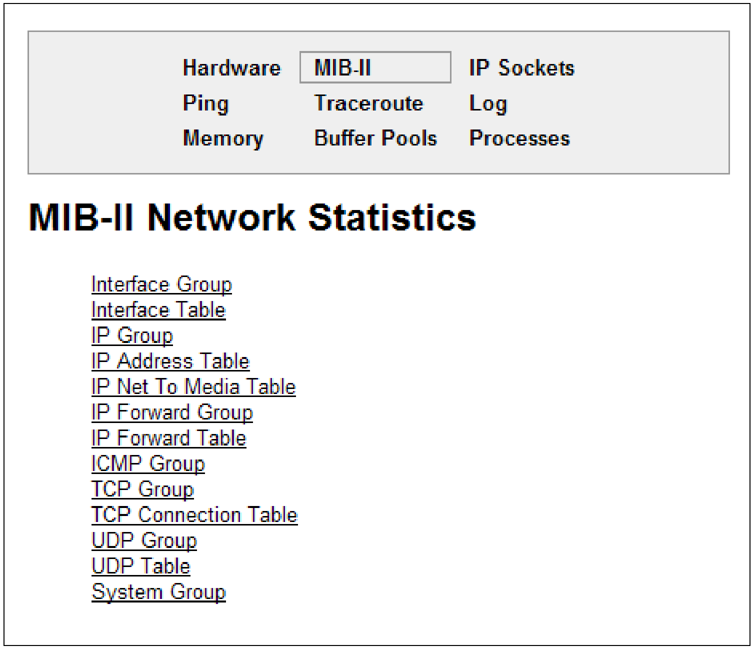
MIB-II Statistics

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

To view MIB-II statistics:

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

Figure 11-16 MIB-II Network Statistics



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

Table 11-17 **Requests for Comments (RFCs)**

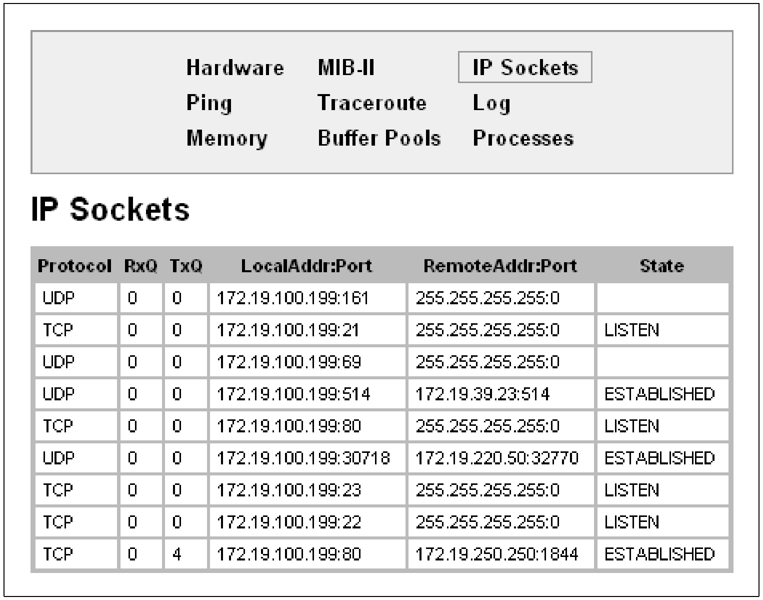
RFC 1213	Original MIB-II definitions.
RFC 2011	Updated definitions for IP and ICMP.
RFC 2012	Updated definitions for TCP.
RFC 2013	Updated definitions for UDP.
RFC 2096	Definitions for IP forwarding.

IP Sockets

To display open IP sockets:

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

Figure 11-18 IP Sockets



IP Sockets

Protocol	RxQ	TxQ	LocalAddr:Port	RemoteAddr:Port	State
UDP	0	0	172.19.100.199:161	255.255.255.255:0	
TCP	0	0	172.19.100.199:21	255.255.255.255:0	LISTEN
UDP	0	0	172.19.100.199:69	255.255.255.255:0	
UDP	0	0	172.19.100.199:514	172.19.39.23:514	ESTABLISHED
TCP	0	0	172.19.100.199:80	255.255.255.255:0	LISTEN
UDP	0	0	172.19.100.199:30718	172.19.220.50:32770	ESTABLISHED
TCP	0	0	172.19.100.199:23	255.255.255.255:0	LISTEN
TCP	0	0	172.19.100.199:22	255.255.255.255:0	LISTEN
TCP	0	4	172.19.100.199:80	172.19.250.250:1844	ESTABLISHED

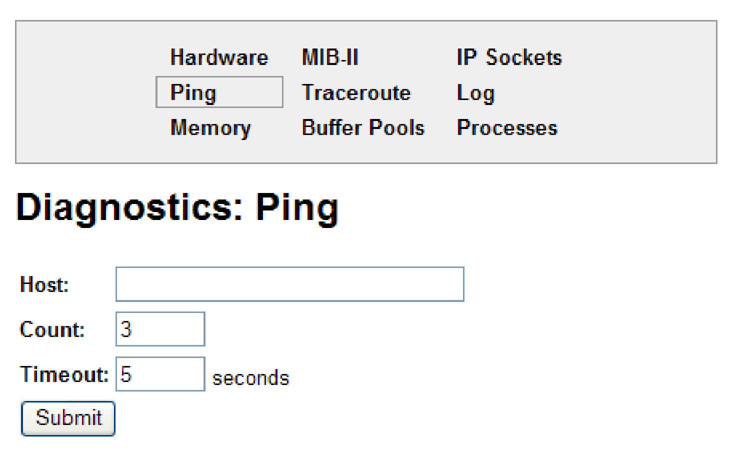
Ping

XPort AR uses 56 bytes of data in a ping packet. Ping size is not configurable.

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 11-19 Diagnostics: Ping



Diagnostics: Ping

Host:

Count: 3

Timeout: 5 seconds

2. Enter or modify the following settings:

Table 11-20 **Diagnostics: Ping**

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

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

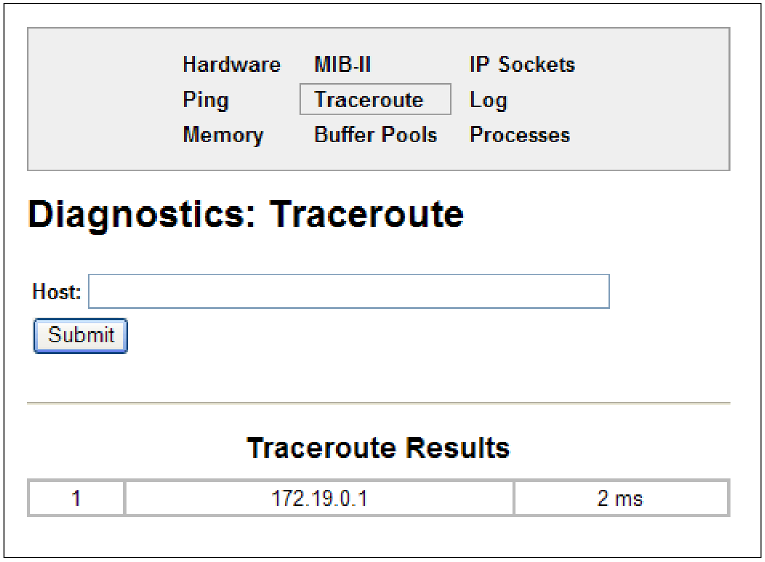
Traceroute

Here you can trace a packet from the XPort 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:

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

Figure 11-21 Diagnostics: Traceroute



1	172.19.0.1	2 ms

2. Enter or modify the following setting:

Table 11-22 **Diagnostics: Traceroute**

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

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

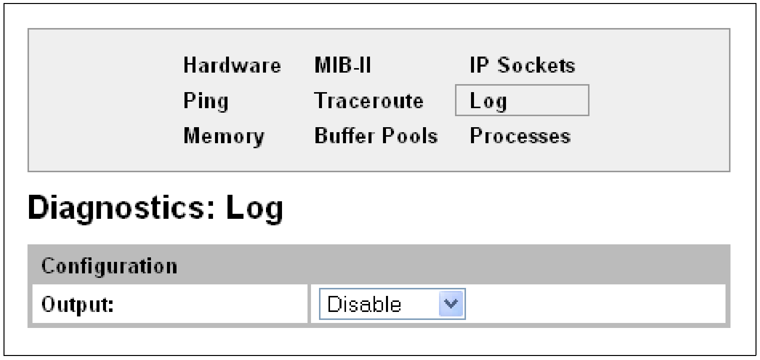
Log

Here you can enable a diagnostics log of configuration items:

To use diagnostics logging:

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

Figure 11-23 Diagnostics: Log

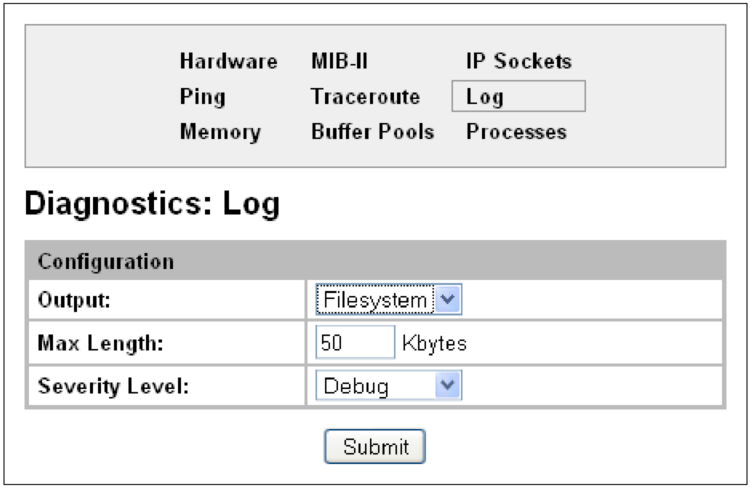


Diagnostics: Log

Configuration	
Output:	Disable

2. Click the **Output** type and select one of the following:
   - Disable (default)
   - Filesystem
   - Line1
   - Line 2
   - Line 3

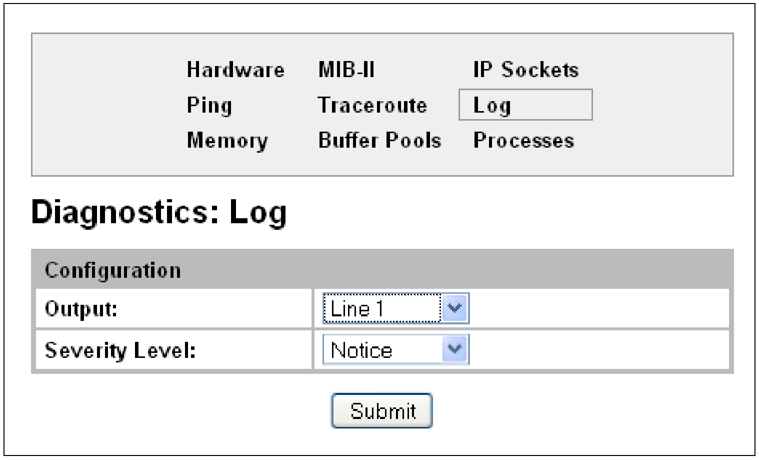
Figure 11-24 Diagnostics: Log (Filesystem)



Diagnostics: Log

Configuration	
Output:	Filesystem
Max Length:	50 Kbytes
Severity Level:	Debug

Figure 11-25 Diagnostics: Log (Line 1)



Diagnostics: Log

Configuration

Output: Line 1

Severity Level: Notice

3. If you selected Filesystem or Line1 Output types also complete additional selections:
   - **Max Length** (for Filesystem only) limits the size in Kbytes of the log (/log.txt).
   - **Severity Level** specifies the level of system message to be logged.
4. Click **Submit**.

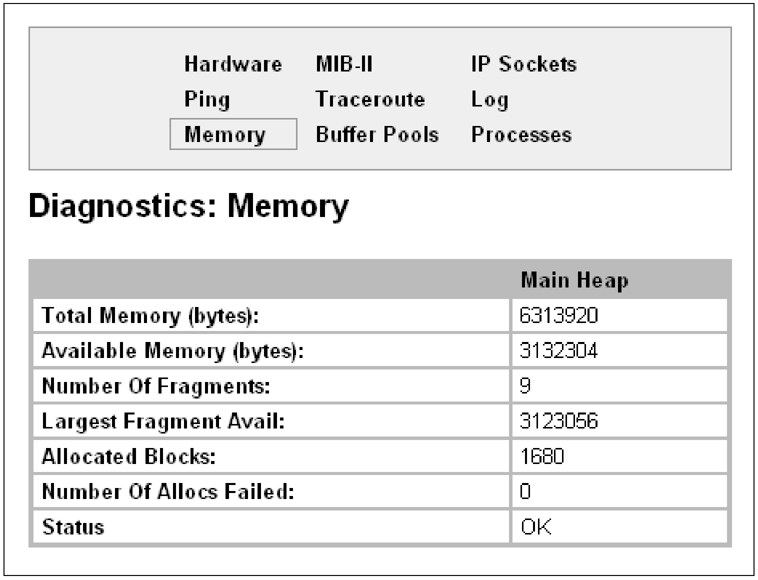
Memory

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

To display memory statistics:

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

Figure 11-26 Diagnostics: Memory



Diagnostics: Memory

	Main Heap
Total Memory (bytes):	6313920
Available Memory (bytes):	3132304
Number Of Fragments:	9
Largest Fragment Avail:	3123056
Allocated Blocks:	1680
Number Of Allocs Failed:	0
Status	OK

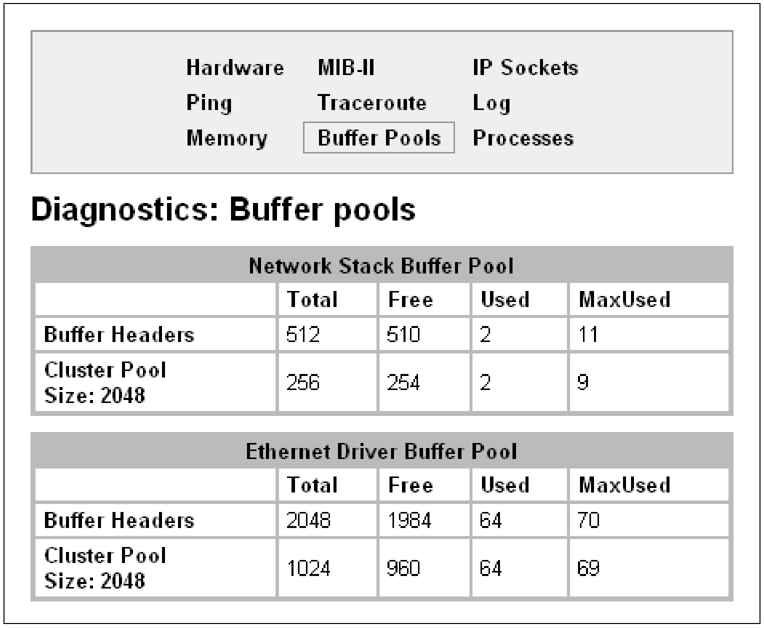
Buffer Pools

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

To display the 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 11-27 Diagnostics: Buffer Pools



Diagnostics: Buffer pools

Network Stack Buffer Pool				
	Total	Free	Used	MaxUsed
Buffer Headers	512	510	2	11
Cluster Pool Size: 2048	256	254	2	9

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

Processes

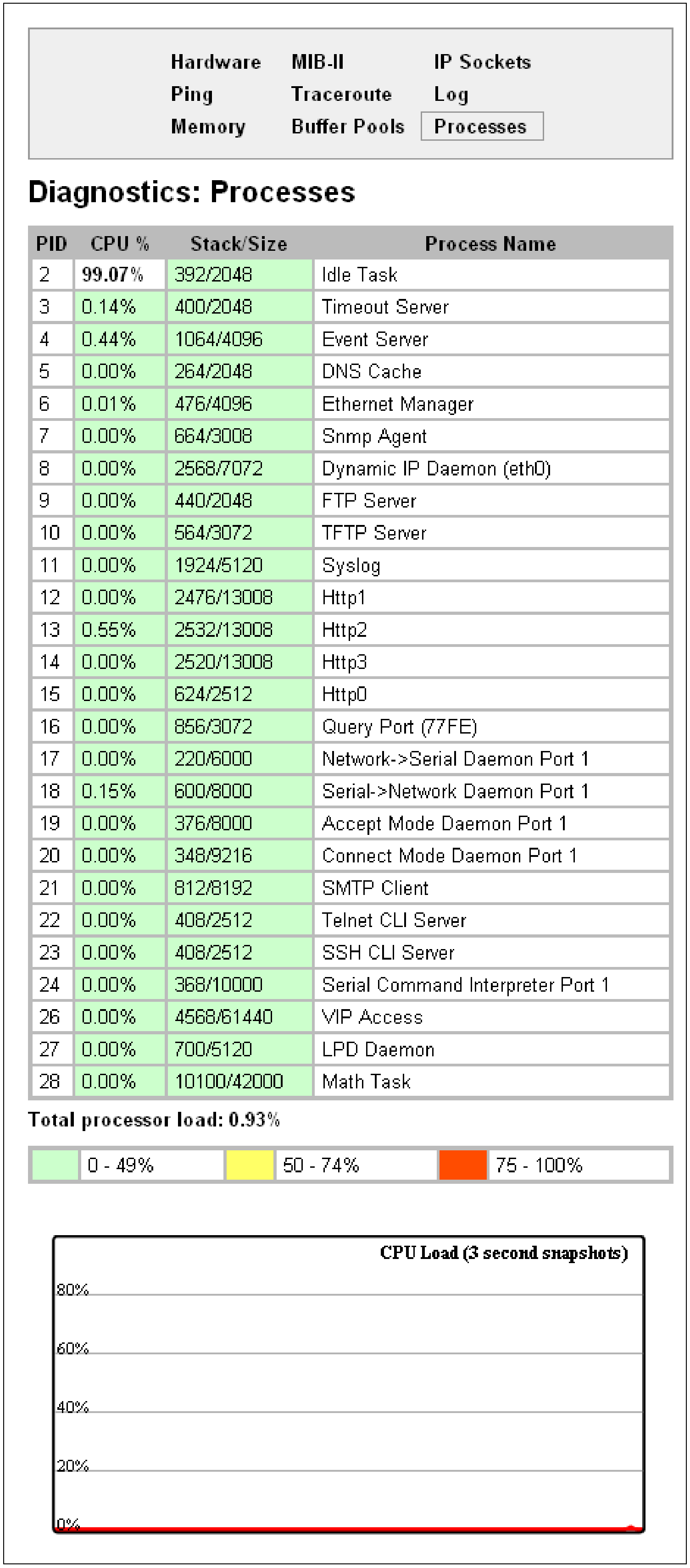
The Processes web page shows all the processes currently running on the system. It shows the Process ID (PID), the percentage of total CPU cycles a process used within the last three seconds, the total stack space available, the maximum amount of stack space used by the process since it started, and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

To display the processes running and their associated statistics:

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

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

Figure 11-28 Diagnostics: Processes



Diagnostics: Processes

PID	CPU %	Stack/Size	Process Name
2	99.07%	392/2048	Idle Task
3	0.14%	400/2048	Timeout Server
4	0.44%	1064/4096	Event Server
5	0.00%	264/2048	DNS Cache
6	0.01%	476/4096	Ethernet Manager
7	0.00%	664/3008	Snmp Agent
8	0.00%	2568/7072	Dynamic IP Daemon (eth0)
9	0.00%	440/2048	FTP Server
10	0.00%	564/3072	TFTP Server
11	0.00%	1924/5120	Syslog
12	0.00%	2476/13008	Http1
13	0.55%	2532/13008	Http2
14	0.00%	2520/13008	Http3
15	0.00%	624/2512	Http0
16	0.00%	856/3072	Query Port (77FE)
17	0.00%	220/6000	Network->Serial Daemon Port 1
18	0.15%	600/8000	Serial->Network Daemon Port 1
19	0.00%	376/8000	Accept Mode Daemon Port 1
20	0.00%	348/9216	Connect Mode Daemon Port 1
21	0.00%	812/8192	SMTP Client
22	0.00%	408/2512	Telnet CLI Server
23	0.00%	408/2512	SSH CLI Server
24	0.00%	368/10000	Serial Command Interpreter Port 1
26	0.00%	4568/61440	VIP Access
27	0.00%	700/5120	LPD Daemon
28	0.00%	10100/42000	Math Task

Total processor load: 0.93%

🟩	0 - 49%	🟨	50 - 74%	🟥	75 - 100%

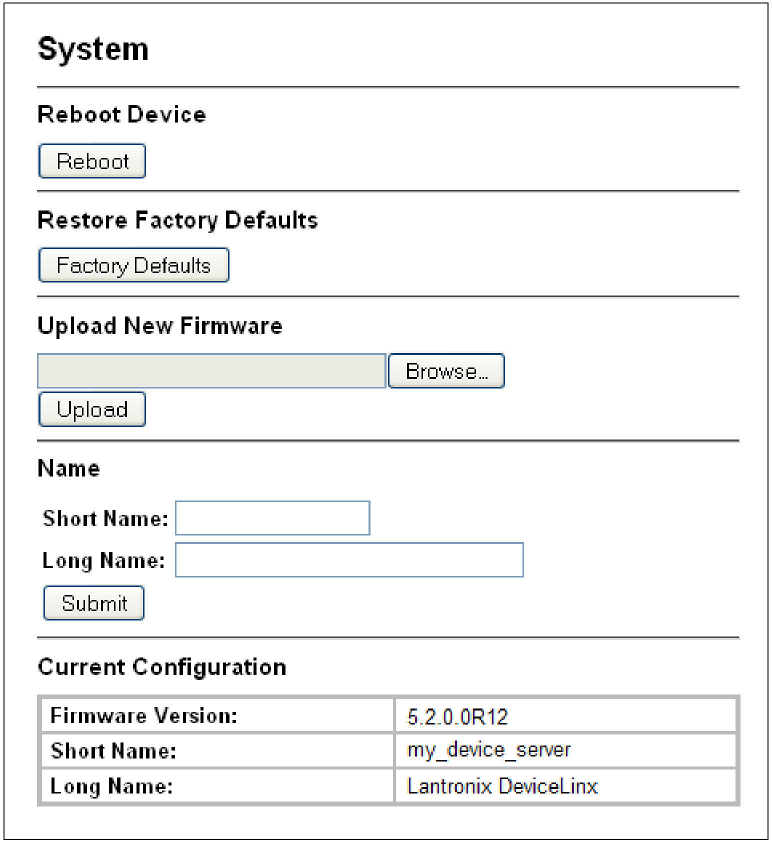
System Settings

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

To configure system settings:

1. Click **System** on the menu bar. The System page opens.

Figure 11-29 System



System

Reboot Device

Restore Factory Defaults

Upload New Firmware

Name

Short Name:

Long Name:

Current Configuration

Firmware Version:	5.2.0.0R12
Short Name:	my_device_server
Long Name:	Lantronix DeviceLinx

2. Configure the following settings:

Table 11-30 **System**

System Settings	Description
Reboot Device	Click **Reboot** to reboot the device. The system refreshes and redirects the browser to the device home page.
Restore Factory Defaults	Click **Factory Defaults** to restore the device to the original factory settings. All configurations will be lost. The device automatically reboots upon setting back to the defaults.

System Settings	Description
Upload New Firmware	Click **Browse** to locate the firmware file location. Click **Upload** to install the firmware on the device. The device automatically reboots upon the installation of new firmware. ***Note:*** *Close and reopen the web manager browser upon a firmware update.*
Name	Enter a new **Short Name** and a **Long Name** (if necessary). The **Short Name** maximum is 32 characters. The **Long Name** maximum is 64 characters. Click **Submit**. Changes take place upon the next reboot.

12: Advanced Settings

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

- *Email Settings*
- *Command Line Interface Settings*
- *XML Settings*

Email Settings

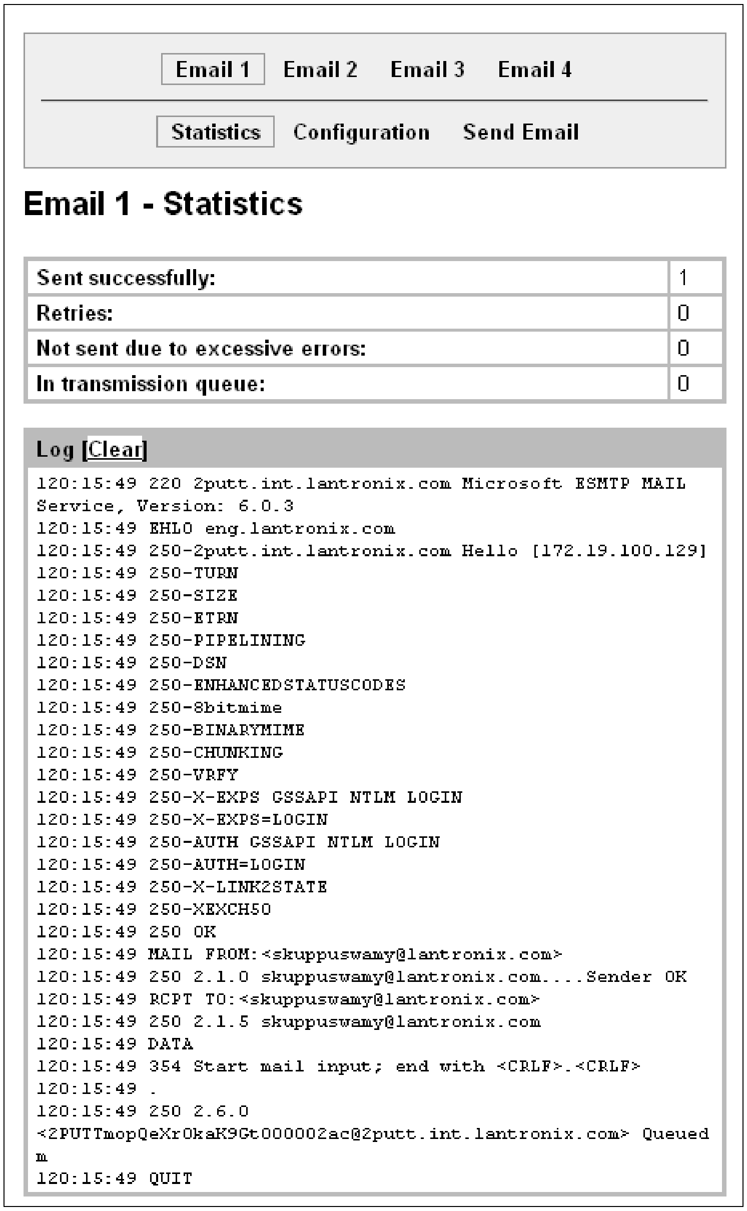
The XPort AR allows you to view and configure email alerts relating to the events occurring within the system. Please see *SMTP Settings on page 96* for additional information.

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

Email Statistics

This read-only page shows various statistics and current usage information about the email subsystem. When you transmit an email, the transmission to the SMTP server gets logged and displayed in the bottom portion of the page.

1. Click **Email 1** and **Statistics** at the top of the page to view its statistics.
2. Click **Clear** to clear the log.



Email 1 - Statistics

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

Log [Clear]

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

Figure 12-1 Email Statistics

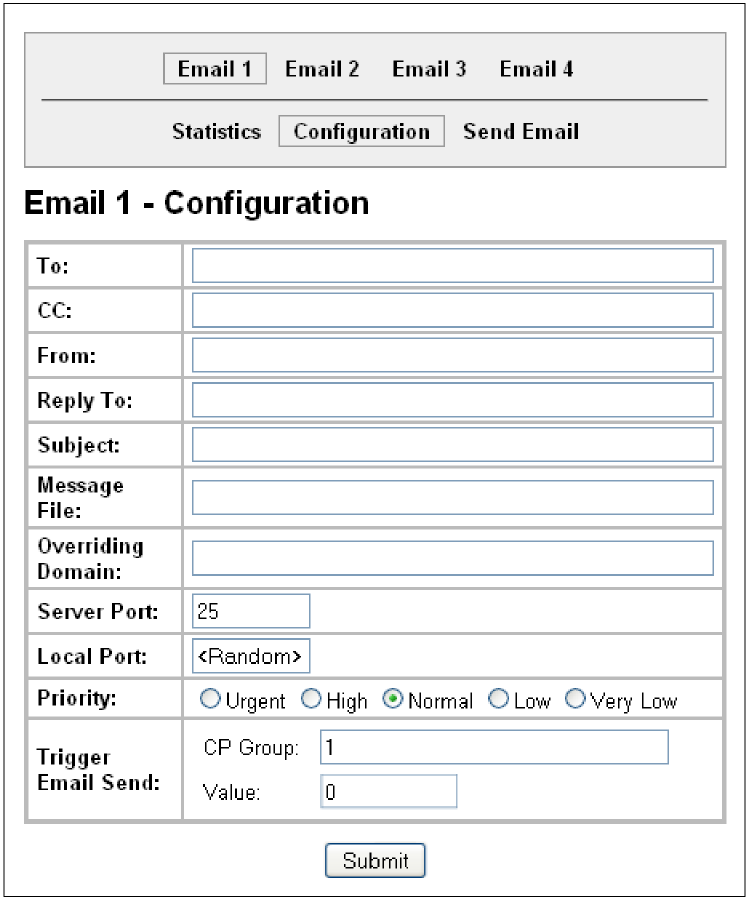
Email Configuration

The XPort AR allows you to view and configure email alerts relating to the events occurring within the system.

To configure email settings:

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

Figure 12-2 Email Configuration



Email 1 - Configuration

To:	
CC:	
From:	
Reply To:	
Subject:	
Message File:	
Overriding Domain:	
Server Port:	25
Local Port:	<Random>
Priority:	○ Urgent ○ High ● Normal ○ Low ○ Very Low
Trigger Email Send:	CP Group: 1 Value: 0

Note: *The **Trigger Email Send** option displayed in the screenshot is only supported in XPort Pro and XPort AR.*

2. Enter or modify the following settings:

Table 12-3 **Email Configuration**

Email – Configuration Settings	Description
To	Enter the email address to which the email alerts will be sent. Multiple addresses are separated by semicolon (;). Required field if an email is to be sent.

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

3. Click **Submit.**
4. To test your configuration, you can send an email immediately by clicking **Send Email** at the top of the page. Refer back to the Statistics page for a log of the transaction.

Command Line Interface Settings

The Command Line Interface (CLI) web page enables you to view statistics about the CLI servers listening on the Telnet and SSH ports and to configure CLI settings.

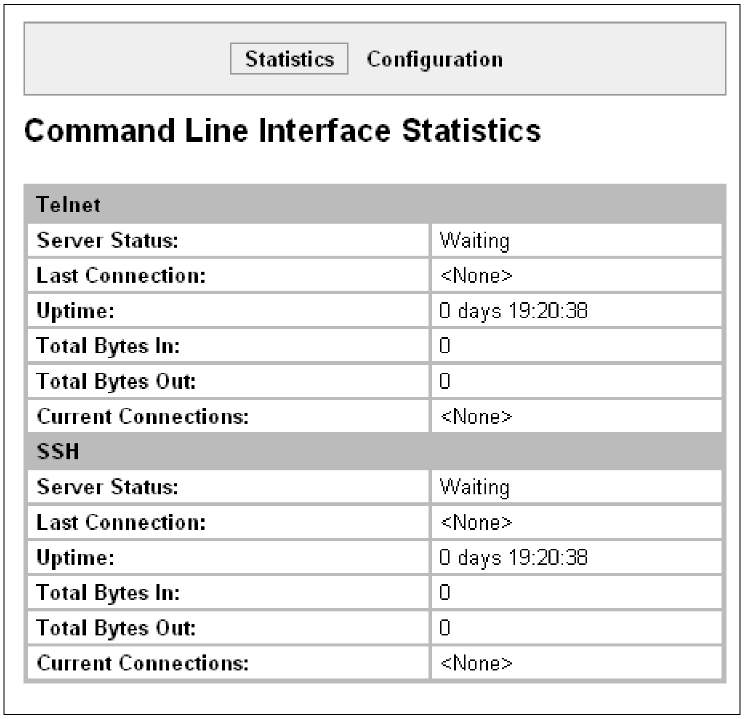
CLI Statistics

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

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

To view the CLI Statistics:

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



Command Line Interface Statistics

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

Figure 12-4 CLI Statistics

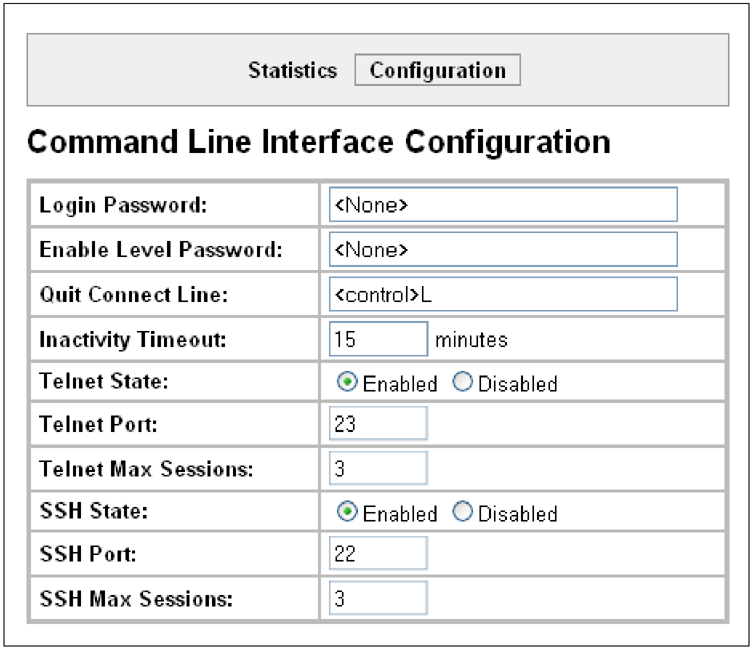
CLI Configuration

On this page you can change CLI 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 appears.

Figure 12-5 CLI Configuration



Command Line Interface Configuration

Login Password:	<None>
Enable Level Password:	<None>
Quit Connect Line:	<control>L
Inactivity Timeout:	15 minutes
Telnet State:	● Enabled ○ Disabled
Telnet Port:	23
Telnet Max Sessions:	3
SSH State:	● Enabled ○ Disabled
SSH Port:	22
SSH Max Sessions:	3

2. Enter or modify the following settings:

Table 12-6 **CLI Configuration**

Command Line Interface Configuration Settings	Description
Login Password	Enter the password for Telnet access.
Enable Level Password	Enter the password for access to the Command Mode Enable level. There is no password by default.
Quit Connect Line	Enter a string to terminate a connect line session and resume the CLI. Type **<control>** before any key the user must press when holding down the **Ctrl** key. An example of such a string is **<control>L.**
Inactivity Timeout	Set an Inactivity Timeout value so the CLI session will disconnect if no data is received after the designated time period. Default is 15 minutes. Enter a value of 0 to disable.
Telnet State	Select **Disabled** to disable Telnet access. Telnet is enabled by default.
Telnet Port	Enter the Telnet port to use for Telnet access. The default is **23**.
Telnet Max Sessions	Maximum number of simultaneous Telnet sessions.
SSH State	Select **Disabled** to disable SSH access. SSH is enabled by default.
SSH Port	Enter the SSH port to use for SSH access. The default is **22**.
SSH Max Sessions	Maximum number of simultaneous SSH sessions.

3. Click **Submit.**

XML Settings

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

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

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

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

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

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

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

Note: *The number of lines available for importing and exporting differ between Lantronix DeviceLinx products. The screenshots in this manual represent one line, as available, for example, on an XPort Pro and EDS1100. However, other device networking products (such as EDS2100, EDS4100, XPort AR, and EDS8/16/32PR) support additional lines and tunnels.*

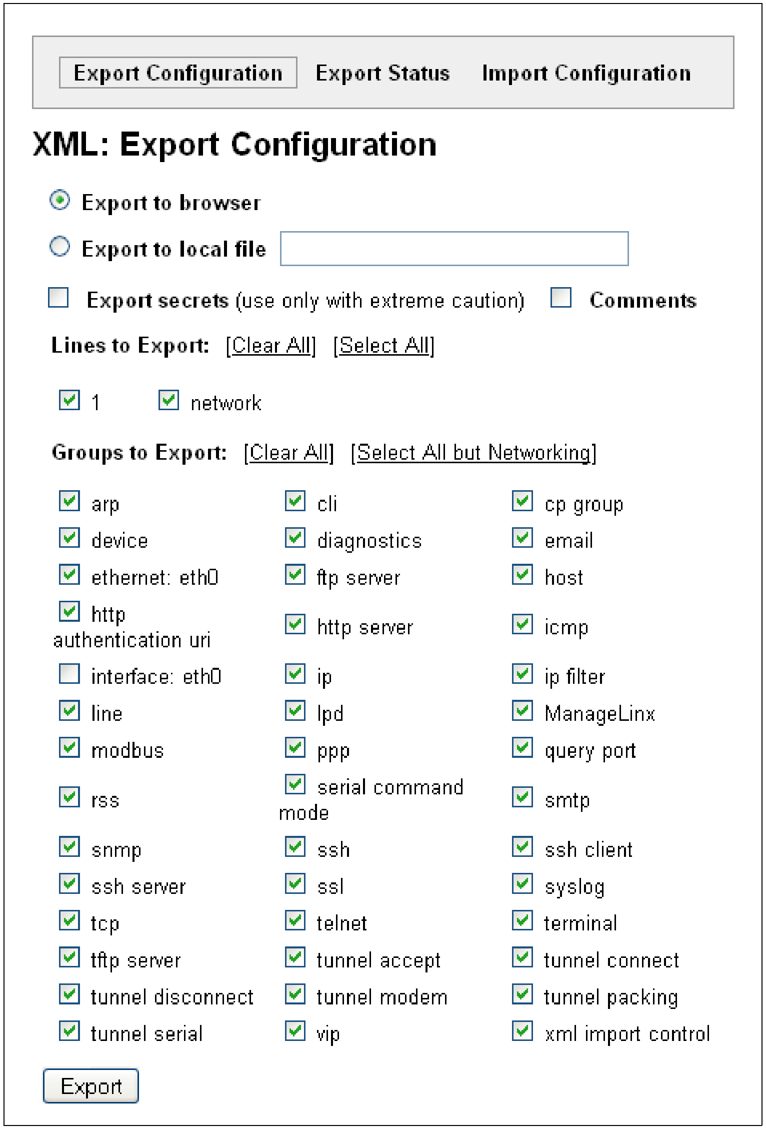
XML: Export Configuration

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

To export the system configuration:

1. Click **XML** on the menu bar. The **XML: Export Configuration** page appears.

Figure 12-7 XML: Export Configuration



XML: Export Configuration

● Export to browser

○ Export to local file

□ Export secrets (use only with extreme caution) □ Comments

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

☑ 1 ☑ network

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

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

2. Enter or modify the following settings:

Table 12-8 **XML Export Configuration**

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

XML Export Configuration Settings (continued)	Description
Lines to Export	Select the instances you want to export in the line, PPP, tunnel, and terminal groups.
Groups to Export	Check the configuration groups that are to be exported to the XML configuration record.

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

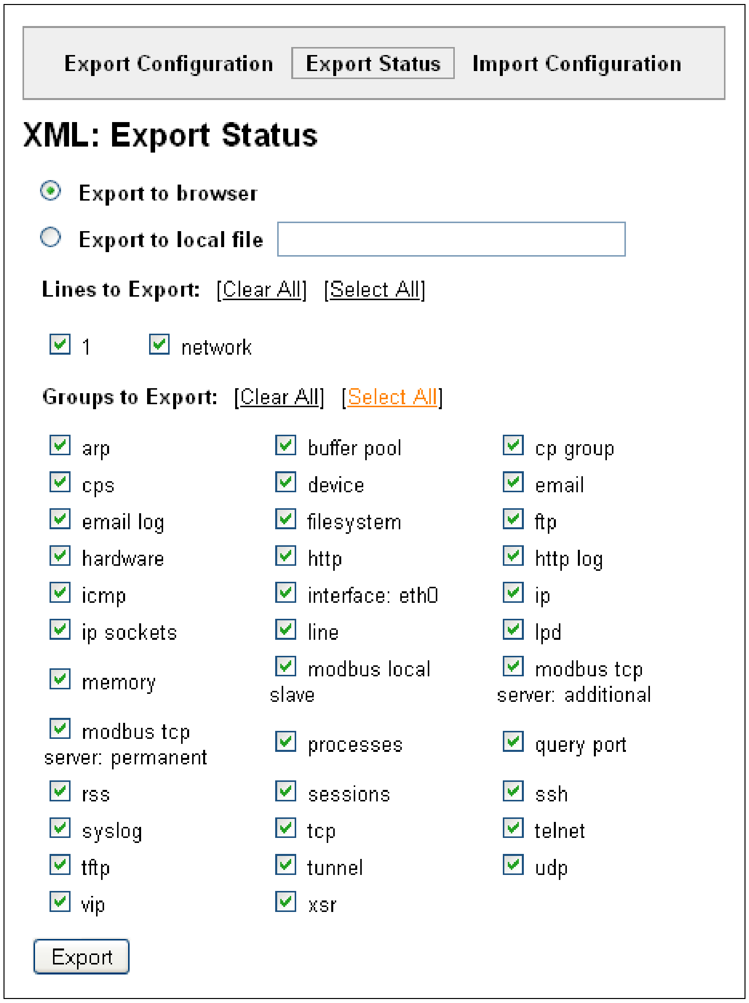
Note: Most browsers will interpret and display the XML data without the XML tags. To view the raw XML, choose the view file source feature of your browser.

XML: Export Status

To export the 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 file system.

1. Click **XML** on menu bar and then **Export Status** at the top of the page. The XML: Export Status page appears.
2. Enter or modify the following settings:



XML: Export Status

● Export to browser

○ Export to local file

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

☑ 1 ☑ network

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

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

Figure 12-9 XML: Export Status

Table 12-10 **XML Export Status**

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

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

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

XML: Import Configuration

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

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

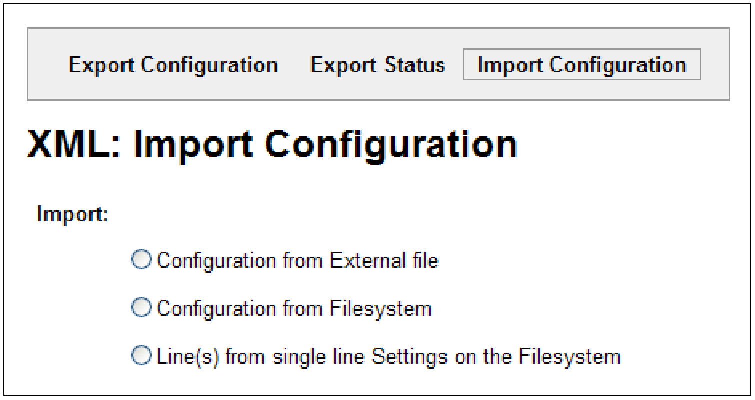
<g>:<i>;<g>:<i>;...

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

To import a system configuration:

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

Figure 12-11 XML: Import Configuration



XML: Import Configuration

Import:

○ Configuration from External file

○ Configuration from Filesystem

○ Line(s) from single line Settings on the Filesystem

2. Click one of the following radio buttons:

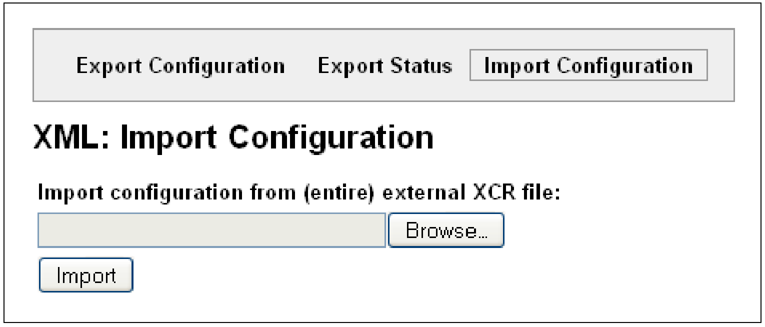
- Configuration from External file. *See Import Configuration from External File on page 120.*

- Configuration from Filesystem. *See Import Configuration from the Filesystem on page 121.*
- Line(s) from single line Settings on the Filesystem. *See Import Line(s) from Single Line Settings on the Filesystem on page 123.*

Import Configuration from External File

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

Figure 12-12 XML: Import Configuration from External File

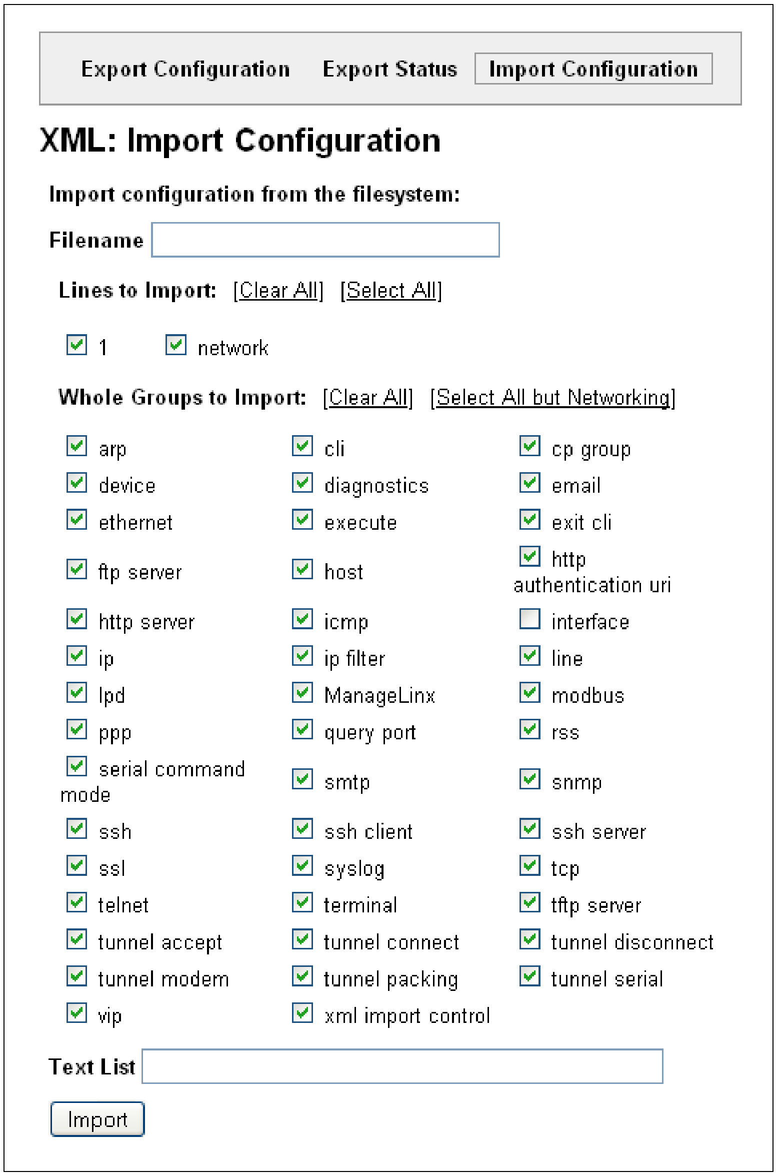


Export Configuration
Export Status
Import Configuration
XML: Import Configuration
Import configuration from (entire) external XCR file:
Browse...
Import

Import Configuration from the Filesystem

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

Figure 12-13 XML: Import from Filesystem



XML: Import Configuration

Import configuration from the filesystem:

Filename

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

☑ 1 ☑ network

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

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

Text List

1. Enter or modify the following settings.

Figure 12-14 XML: Import Configuration from Filesystem

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

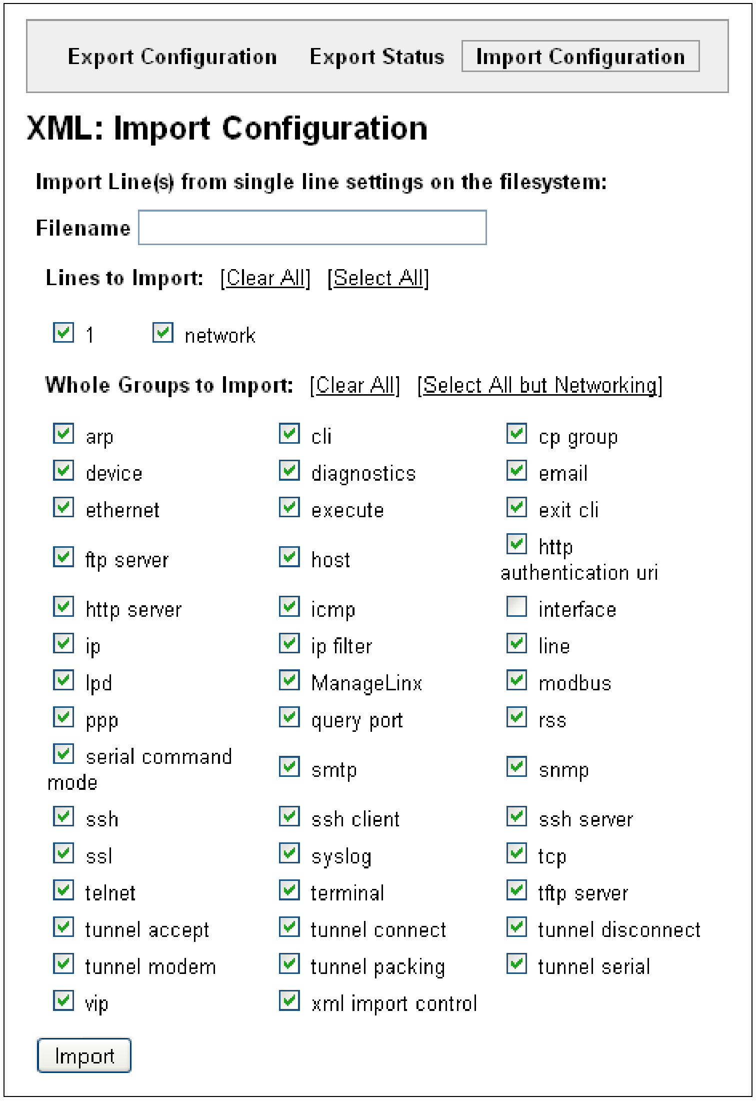
2. Click **Import**.

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

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

To modify Single Line Settings on the Filesystem:

Figure 12-15 XML: Import Line(s) from Single Line Settings on the Filesystem



XML: Import Configuration

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

Filename

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

☑ 1 ☑ network

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

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

1. Enter of modify the following settings:

Table 12-16 **XML: Import Line(s) from Single Line Settings**

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

2. Click **Import**.

13: Branding the XPort AR

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

- *Web Manager Customization*
- *Short and Long Name Customization*

Web Manager Customization

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

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

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

1. FTP to the XPort AR device.
2. Make a directory (**mkdir**) and name it http/config
3. Change to the directory (**cd**) that you created in step 2. (http/config)
4. Get the file by using **get** <filename>
5. Modify the file as required or create a new one with the same name
6. Put the file by using **put** <filename>
7. Type **quit**. The overriding files appear in the file system's http/config directory.
8. Restart any open browser to view the changes.
9. If you wish to go back to the default files in the firmware image, simply delete the overriding files from the file system.

Short and Long Name Customization

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

```
(enable)# show
```

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

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

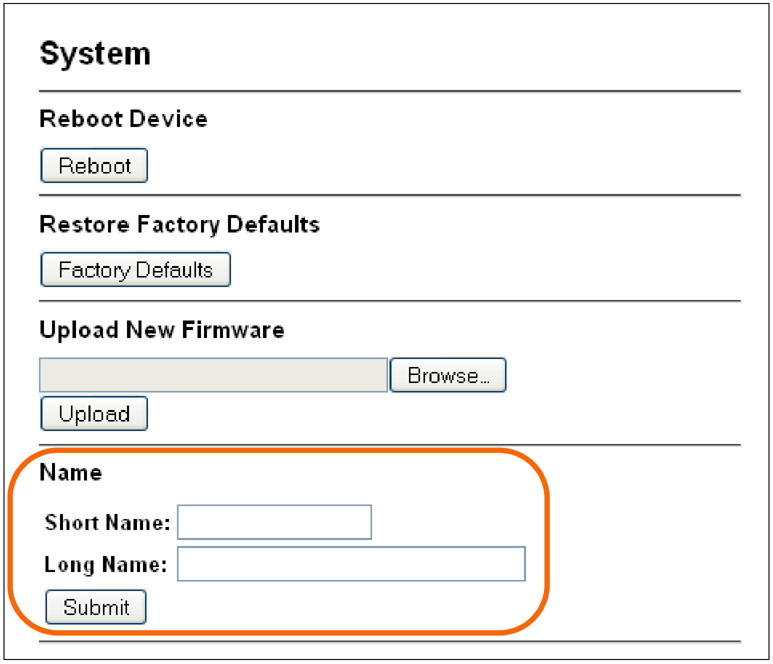
For example:

```
(enable)# show XPort

Product Information:

Product Type: Lantronix XPort AR (XPort)
```

To change the short and long names with the web manager:

1. Click **System** in the menu bar. The System page opens.

Figure 13-1 System Branding



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

14: Updating Firmware

Obtaining Firmware

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

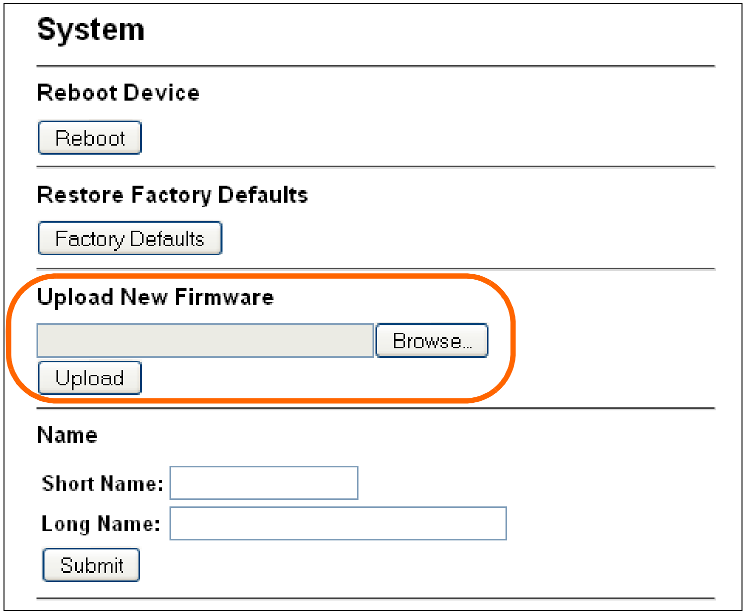
Loading New Firmware

Reload the firmware using the device web manager Filesystem page.

To upload new firmware:

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

Figure 14-1 Update Firmware



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

Note: *Alternatively, firmware may be updated by sending the file to the XPort AR over a FTP or TFTP connection.*

Appendix - Technical Support

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

Technical Support US

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

Technical Support Europe, Middle East, Africa

Phone: +33 13 930 4172
Email: eu_techsupp@lantronix.com or eu_support@lantronix.com

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

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

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

Appendix - Binary to Hexadecimal Conversions

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

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

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

Converting Binary to Hexadecimal

Conversion Table

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

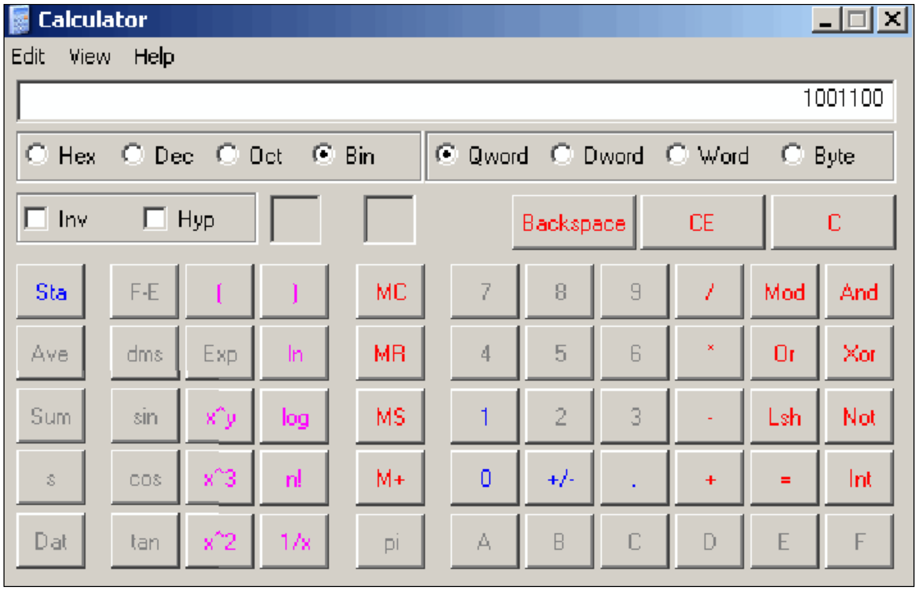
Table 16-1 **Binary to Hexadecimal Conversion Table**

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

Scientific Calculator

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

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



Calculator

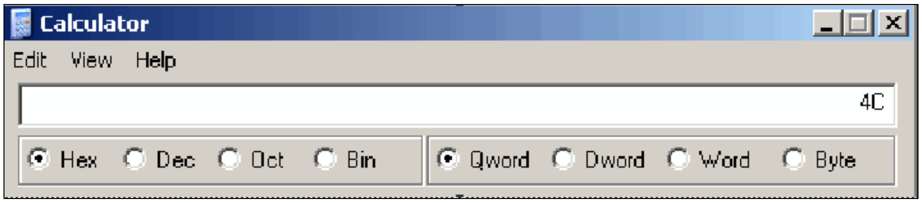
1001100

○ Hex ○ Dec ○ Oct ● Bin

● Qword ○ Dword ○ Word ○ Byte

□ Inv □ Hyp

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



Calculator

4C

● Hex ○ Dec ○ Oct ○ Bin

● Qword ○ Dword ○ Word ○ Byte

Appendix - Compliance

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

Manufacturer's Name & Address:

Lantronix 167 Technology Drive, Irvine, CA 92618 USA

Product Name Model:

XPort AR Embedded Device Server

Conforms to the following standards or other normative documents:

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

Immunity

EN55024: 1998 + A1: 2001 + A2: 2003

Direct & Indirect ESD

EN61000-4-2: 1995

RF Electromagnetic Field Immunity

EN61000-4-3: 2002

Electrical Fast Transient/Burst Immunity

EN61000-4-4: 2004

Surge Immunity

EN61000-4-5: 2006

RF Common Mode Conducted Susceptibility

EN61000-4-6: 1996

Power Frequency Magnetic Field Immunity

EN61000-4-8: 1994

Voltage Dips and Interrupts

EN61000-4-11: 2004

Safety

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

Manufacturer's Contact:

Lantronix
167 Technology Drive, Irvine, CA 92618 USA
Tel: 949-453-3990
Fax: 949-450-7249

RoHS Notice

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

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

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

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

Index