LANTRONIX®

XPort™ AR ARCHITECT

XPort AR
User Guide

Part Number 900-405
Revision C December 2006

Copyright & Trademark

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

Contacts

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

Technical Support
Phone: 800-422-7044 or 949-453-7198
Fax: 949-450-7226
Online: www.lantronix.com/support

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

Disclaimer & Revisions

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

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

Date	Rev.	Comments
6/2005	A	Initial Document
11/2005	B	Added V2.0 software information
12/2006	C	Added V3.0 information

Contents

Figures

1: Using This Guide

Purpose and Audience

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.

Summary of Chapters

The remaining chapters in this guide include:

Chapter	Description
2: Description and Specifications	Main features of the product and the protocols it supports. Includes technical specifications.
3:Using DeviceInstaller	Instructions for viewing the current configuration using DeviceInstaller.
4:Configuration Using Web Manager	Instructions for accessing Web Manager and using it to configure settings for the XPort AR.
5:Point-to-Point Protocol (PPP)	Overviews PPP on the XPort AR.
6:Tunneling	Information on tunneling features available on the serial lines.
7:SSH and SSL Security	Overview and configuration of SSH and SSL security settings.
8:Using Email	Information on the SMTP server and setting email parameters on the XPort AR.
9:Configuration Pin Manager	Information on the Configuration Pin Manager (CPM) and setting the configurable pins to work with a device.
10:XML	Configuring the XPort AR using XML.
11:Branding the XPort AR	Instructions for customizing the XPort AR.
12:Updating Firmware	Instructions for obtaining the latest firmware and updating the XPort AR.
A: Technical Support	How to contact Lantronix Technical Support.
B: Binary to Hexadecimal	Instructions for converting binary values to hexadecimal and tables listing all configuration options in hexadecimal notation.

Additional Documentation

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

XPort AR Getting Started	Provides the steps for getting the XPort AR evaluation board up and running.
XPort AR Integration Guide	Provides information about the XPort AR hardware, testing the XPort AR using the evaluation board, and integrating the XPort AR into your product.
XPort AR Command Reference	Instructions for accessing Command Mode (the command line interface) using a Telnet connection through the network or through the serial port. Detailed information about the commands.

2: Description and Specifications

This chapter summarizes the XPort AR device server's features and basic information needed before getting started.

Features

The XPort AR is designed with additional features above and beyond the original XPort, including:

- The Evolution OS operating system
- Two full serial ports with all hardware handshaking signals or three serial ports without handshaking signals
- 11 configurable pins
- Supports fully compliant PoE designs by using PoE compliant magnetics and passing through both the used and unused pairs
- Increased memory: 4MB Flash and 1.25MB RAM
- Hardware capability in place to allow future software support for:
  - I2C Bus
  - SPI Bus
  - CAN Bus
  - USB
  - External interrupts, including one non-maskable
  - Timer input

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 units
- Telecommunications equipment
- Data display devices
- Security alarms and access control devices
- Handheld instruments
- Modems

- Time/attendance clocks and terminals

Protocol Support

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

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

Evolution OS™

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

- Built-in Web server for configuration and troubleshooting from Web-based browsers
- CLI configurability
- SNMP management
- XML data transport and configurability
- Rich Site Summary (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.

Power over Ethernet (PoE)

The XPort AR supports PoE (also known as the IEEE standard 802.3af). Conventionally, network devices require a connection to the network and a power connection. PoE provides power to network devices over an Ethernet connection if the required hardware is available. The XPort AR passes PoE through the RJ45 to a connector on the bottom. To enable PoE, take the connections and design a PoE circuit and regulator to provide power for the device connected to the XPort AR. The XPort AR passes power not only through unused pairs, but through communications pairs as well.

Web-Based Configuration and Troubleshooting

Built upon popular Internet-based standards, the XPort AR enables users to configure, manage, and troubleshoot efficiently through a simplified browser-based interface that can be accessed anytime from anywhere. All configuration and troubleshooting options are launched from a well-organized, multi-page interface. Users can access all functionality via a Web browser, allowing them flexibility and remote access. As a result, users can enjoy the advantages of decreased downtime (based on the troubleshooting tools) and the ability to implement configuration changes easily (based on the configuration tools).

Command-Line Interface (CLI)

Making the edge-to-enterprise vision a reality, the 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 makes device configuration transparent to users and administrators. The XML is easily editable with a standard text or XML editor.

Rich Site Summary (RSS)

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

Enterprise-Grade Security

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

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

SSH and SSL can:

- Verify the data received came from the proper source

- Validate that the data transferred from the source over the network has not changed when it arrives at its destination (shared secret and hashing)
- Encrypt data to protect it from prying eyes and nefarious individuals
- Provide the ability to run popular M2M protocols over a secure SSH 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 can not be used to bring down other devices on the network.

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

Troubleshooting Capabilities

The 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 three basic methods for logging into the XPort AR and assigning IP addresses and other configurable settings:

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

Web Manager: Through a web browser, configure the XPort AR's settings using the Lantronix Web Manager. (See *4:Configuration Using Web Manager*.)

Command Mode: There are two methods to accessing Command Mode: making a Telnet connection or connecting a terminal (or a PC running a terminal emulation program) to the unit's serial port. (See the XPort AR Command Reference Guide for Command Mode input and available 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: 0x77FE Query port
- TCP/UDP Port 1001: Tunnel 1
- TCP/UDP Port 1002: Tunnel 2

Product Information Label

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

- Bar code
- Serial number
- Product ID (name)
- Part number

- Hardware address (MAC address)

Figure 2-2. Product Label

3: Using DeviceInstaller

This chapter covers the steps for viewing the XPort AR device server's properties and device details.

Accessing XPort AR using DeviceInstaller

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

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

1. Click **Start→Programs → Lantronix→DeviceInstaller→DeviceInstaller**.
2. Click on the XPort AR folder. The list of Lantronix XPort AR devices available displays.
3. Expand the list of XPorts by clicking the **+** symbol next to the XPort AR icon. Select the XPort AR unit by clicking on its IP address to view its configuration.

Viewing the XPort AR's Current Configuration

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

Name	Configurable field. Enter a **name** to identify the XPort AR. Double-click on the field, type in the value, and press **Enter** to complete. This name is not visible on other PCs or laptops using DeviceInstaller.
Group	Configurable field. Enter a **group** to categorize the XPort AR. Double-click on the field, type in the value, and press **Enter** to complete. This group name is not visible on other PCs or laptops using DeviceInstaller.
Comments	Configurable field. Enter **comments** for the XPort AR. Double-click on the field, type in the value, and press **Enter** to complete. This description or comment is not visible on other PCs or laptops using DeviceInstaller.
Device Family	Non-configurable field. Displays the XPort AR's device family type as **XPort AR**.
Type	Non-configurable field. Displays the device type as **XPort AR**.
ID	Non-configurable field. Displays the XPort AR's ID embedded within the box.
Hardware Address	Non-configurable field. Displays the XPort AR's hardware (or MAC) address.
Firmware Version	Non-configurable field. Displays the firmware currently installed on the XPort AR.

Extended Firmware Version	Provides additional information on the firmware version.
Online Status	Non-configurable field. Displays the XPort AR's status as online, offline, unreachable (the XPort AR is on a different subnet), or busy (the XPort AR is currently performing a task).
Telnet Enabled	Displays whether Telnet is enabled on this XPort AR.
Telnet Port	Non-configurable field. Displays the XPort AR's port for telnet sessions.
Web Enabled	Displays whether Web Manager access is enabled on this XPort AR.
WebPort	Non-configurable field. Displays the XPort AR's port for Web Manager configuration.
Maximum Baud Rate Supported	Non-configurable field. Displays the XPort AR's maximum baud rate. ***Note:*** *the XPort AR may not currently be running at this rate.*
Firmware Upgradeable	Non-configurable field. Displays **True**, indicating the XPort AR's firmware is upgradeable as newer version become available.
IP Address	Displays the XPort AR's current IP address. To change the IP address, click on the **Assign IP** button on the DeviceInstaller menu bar.
Supports Configurable Pins	Non-configurable field. Displays **True**, indicating configurable pins are available on the XPort AR.
Supports Email Triggers	Non-configurable field. Displays **True**, indicating email triggers are available on the XPort AR.

4: Configuration Using Web Manager

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

Accessing Web Manager through a Web Browser

Log into the XPort AR using a standard Web browser.

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

To access Web Manager:

1. Open a standard web browser (such as Netscape Navigator 6.x and above, Internet Explorer 5.5. and above, Mozilla Suite, Mozilla Firefox, or Opera).

2. Enter the IP address of the XPort AR in the address bar. The XPort AR's built-in security requires you to log in with your user name and password.

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

3. The Web Manager home page displays.

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

Figure 4-1. Web Manager Home Page

Network Settings

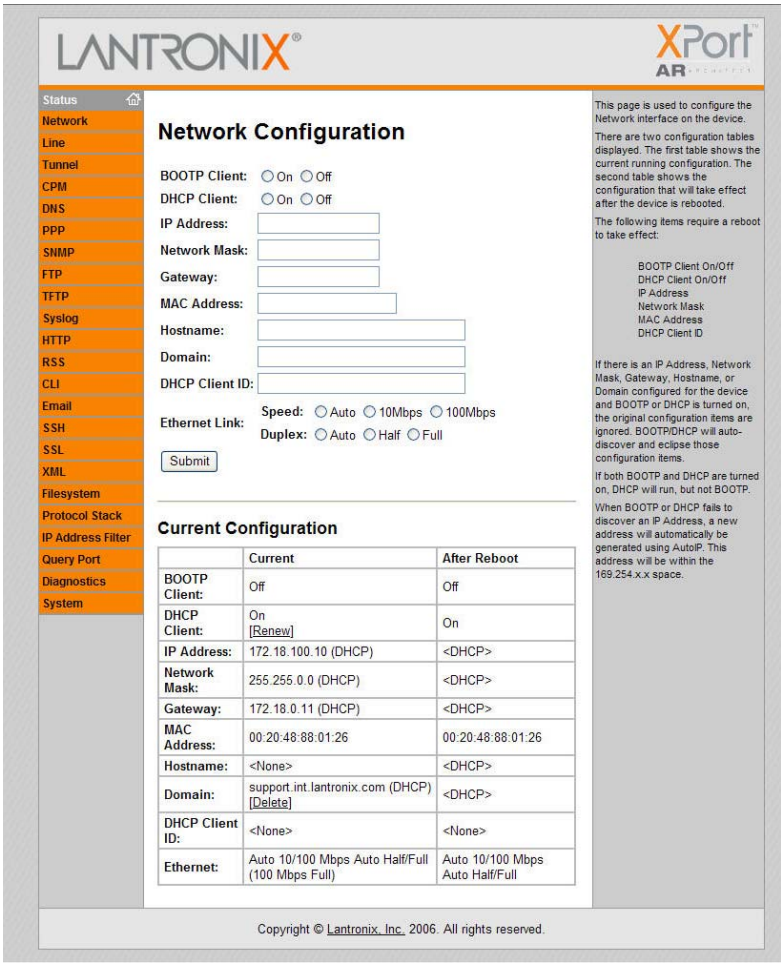
Click the **Network** link on the left navigation bar to display the Network menu. The sub-menus displayed allow for the configuration of the general network settings, protocol stack, DNS, SNMP, FTP, TFTP, IP address filter, and the query port.

Network Configuration

To configure the network's general configuration:

1. Click **Network → Configuration** from the navigation menu. The Network Configuration window displays.

Figure 4-2. Network Configuration



2. Enter or modify the following fields:

BOOTP Client	Select On or Off. Overrides the configured IP address, network mask, gateway, hostname, and domain. Note: When DHCP is set to On, the system automatically uses DHCP, regardless if BOOTP Client is set to On.
DHCP Client	Select On, Off, or Renew. Overrides the configured IP address, network mask, gateway, hostname, and domain.
IP Address	Enter the XPort AR's static IP address. The static address is used when BOOTP and DHCP are both set to Off.
Network Mask	Enter the XPort AR's network mask.
Gateway	Enter the XPort AR's gateway address.
MAC Address	Enter the XPort AR's new MAC address.
Hostname	Enter the unit's hostname.
Domain	Enter the unit's domain name.

DHCP Client ID	Enter the ID if a DHCP ID is used by the DHCP server. The DHCP server's lease table displays IP addresses and MAC addresses for devices. The lease table displays the Client ID, in hexadecimal notation, instead of the XPort AR's MAC address.
Ethernet	Select the speed for Ethernet transmission.

3. In the **Current Running Configuration** table, delete currently stored fields as necessary.
4. Click **Submit**. Changes are applied immediately to the XPort AR. Changes to the following settings require a reboot for the changes to take effect: DHCP, BOOTP, IP address, network mask, gateway, MAC address, and DHCP client ID.

Note: *If DHCP or BOOTP fails, AutoIP intervenes and assigns an address. In this case, the static IP (if configured) is ignored.*

Line 1, Line 2, and Line 3 Settings

Select the **Line 1**, **Line 2**, or **Line 3** link on the left menu bar to display the **Line** menu. The sub-menus allow for both general configuration and command mode configuration.

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

Line 1 Configuration

To configure Line 1:

1. Click **Line 1** → **Configuration** from the navigation menu. The Line 1 Configuration window displays.

Figure 4-3. Line 1 Configuration

2. Enter or modify the following fields:

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

Xoff Char	When **Flow Control** is set to **Software**, specify **Xoff char**. Prefix a decimal character with **** or a hexadecimal character with 0x, or provide a single printable character. The default Xoff char is 0x13.

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

Line 1 Command Mode

Setting Command Mode enables the CLI on the serial line.

To configure Line 1's command mode:

1. Click **Line 1 → Command Mode** from the navigation menu. The Line 1 Command Mode window displays.

Figure 4-4. Line 1 Command Mode

2. Enter or modify the following fields:

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** starts command mode based on the value of a CP group. **Use both Serial String and CP Group** enables command mode when both the serial string is read and the appropriate CP group value is communicated. **Disabled** turns off command mode.
Wait Time	Enter the wait time for the serial string during boot-up.

Serial String	In the **Char** field, enter the serial string characters. Select the string type from the pull down menu as **Character**, **Binary**, or **Decimal** notation.
Echo Serial String	Select **Yes** to enable echoing of the serial string at boot-up.
CP Group	Enter the CP group name and its value.
Signon Message	In the **Char** field, enter the boot-up signon message. Select the string type from the pull down menu as **Character**, **Binary**, or **Decimal** notation.

3. In the **Current Configuration** table, clear currently stored fields as necessary.
4. Click **Submit**. Changes are applied immediately to the XPort AR.

Tunnel 1 and Tunnel 2 Settings

Select the **Tunnel 1** or **Tunnel 2** link on the left menu bar to display the **Tunnel** menu. The sub-menus allow for the configuration of serial settings, connect mode, accept mode, disconnect mode, packing mode, start and stop characters, and modem emulation.

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

Figure 4-5. Tunnel 1

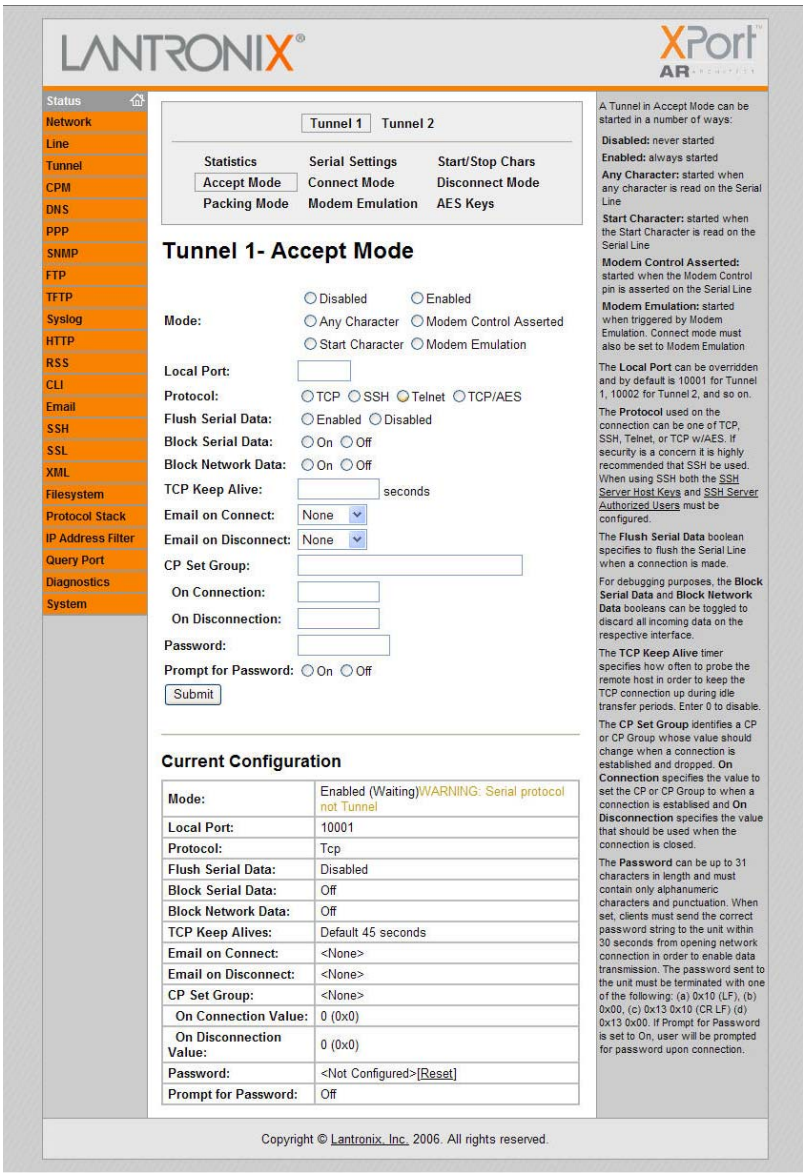
Accept Mode

In accept mode, the XPort AR listens (waits) for incoming connections.

To configure the tunnel's accept mode:

1. Click **Tunnel 1 → Accept Mode** from the navigation menu. The Tunnel 1 Accept Mode window displays.

Figure 4-6. Tunnel 1 Accept Mode



2. Enter or modify the following fields:

Mode	Select the method used to start a tunnel in Accept mode. Choices are: **Disabled** = do not accept an incoming connection. **Enabled** = accept an incoming connection. (*default*) **Any Character** = start waiting for an incoming connection when any character is read on the serial line.

	Start Character = start waiting for an incoming connection when the start character for the selected tunnel is read on the serial line. **Modem Control Asserted** = start waiting for an incoming connection as long as the Modem Control pin (DSR) is asserted on the serial line until a connection is made. **Modem Emulation** = start waiting for an incoming connection when triggered by modem emulation AT commands. Connect mode must also be set to **Modem Emulation.**
Local Port	Enter the port number for use as the local port. The default is port 10001.
Protocol	Select the protocol type for use with Accept Mode. The default protocol is TCP.
Flush Serial Data	Select **Enabled** to flush the serial data buffer on a new connection.
Block Serial Data	Select **On** to block, or not tunnel, serial data transmitted to the XPort AR.
Block Network Data	Select **On** to block, or not tunnel, network data transmitted to the XPort AR.
TCP Keep Alive	Enter the time, in milliseconds, the unit 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.
CP Set Group	Identifies a CP or CP Group whose value should change when a connection is established and dropped.
On Connection	Specifies the value to set the CP or CP Group when a connection is established.
On Disconnection	Specifies the value used when the connection is closed.
Password	Enter a password that clients must send to the EDS 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 XPort AR must be terminated with one of the following: (a) 0x10 (LF), (b) 0x00, (c) 0x13 0x10 (CR LF), or (d) 0x13 0x00.
Prompt for Password	Indicate whether the user should be prompted for the password upon connection. **On** = prompt for a password upon connection. **Off** = do not prompt for a password upon connection.

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

Packing Mode

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

To configure the tunnel's packing mode:

1. Select **Tunnel 1 → Packing Mode** from the navigation menu. The Tunnel 1 Packing Mode window displays.

Figure 4-7. Tunnel 1 Packing Mode

2. Enter or modify the following fields:

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

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

Serial Settings

To configure serial settings:

1. Click **Tunnel 1 → Serial Settings** from the navigation menu. The Tunnel 1 Serial Settings window displays.

Figure 4-8. Tunnel 1 Serial Settings

2. Enter or modify the following fields:

Buffer Size	Enter the buffer size used for the tunneling of data received.
Read Timeout	Enter the time, in milliseconds, for tunneling wait for serial data
Wait for Read Timeout	Select **Enabled** to cause the tunneling to wait for a read timeout before returning serial data.

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

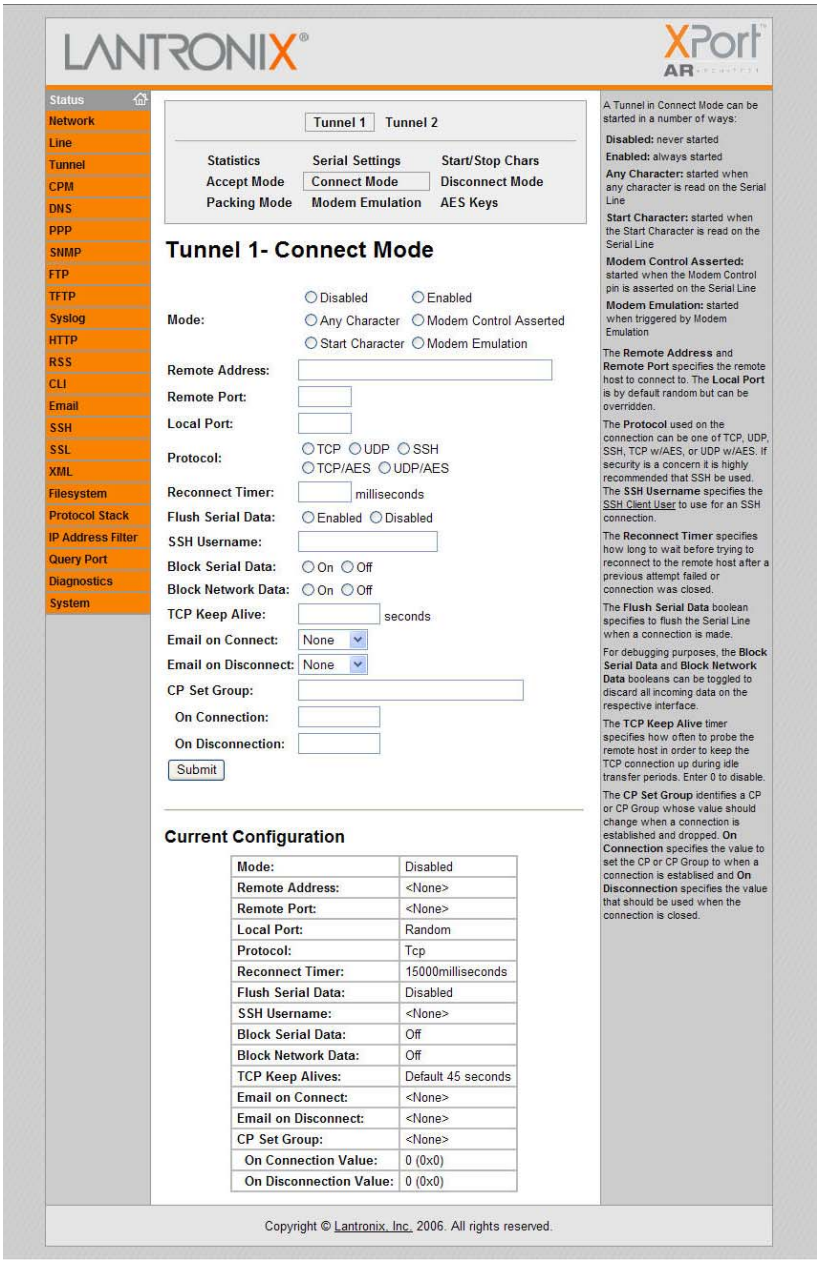
Connect Mode

Connect mode defines how the unit makes an outgoing connection.

To configure Tunnel 1's connect mode:

1. Select **Tunnel 1 → Connect Mode** from the navigation menu. The Tunnel 1 Connect Mode window displays.

Figure 4-9. Tunnel 1 Connect Mode



2. Enter or modify the following fields:

Mode	Select **Disabled** to turn off connect mode. **Any Character** enables connect mode upon receiving a character. **Start Character** enables connect mode upon receiving the start character. Select **Modem CTRL Assert** to enable connect mode when the modem control pin (DSR pin) is asserted on the serial line. Select **Modem Emulation** to use modem emulation on this tunnel.
Remote Address	Enter the remote address to which the XPort AR will connect. Enter an IP address or DNS name.
Remote Port	Enter the remote port number.
Local Port	Enter the port for use as the local port. A random port is selected by default.
Protocol	Select the protocol type for use in command mode. TCP is the default protocol.
Reconnect Timer	Enter the reconnect time in milliseconds. The XPort AR attempts to reconnect this amount of time after failing a connection or exiting an existing connection.
SSH Username	Enter the SSH username. The tunnel uses the SSH keys for the client username.
Block Serial Data	Select **On** to block (not tunnel) serial data transmitted to the XPort AR.
Block Network Data	Select **On** to block (not tunnel) network data transmitted to the XPort AR.
TCP Keep Alive	Enter the time, in milliseconds, the unit 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.
CP Set Group	Identifies a CP or CP Group whose value should change when a connection is established and dropped.
On Connection	Specifies the value to set the CP or CP Group when a connection is established.
On Disconnection	Specifies the value used when the connection is closed.

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

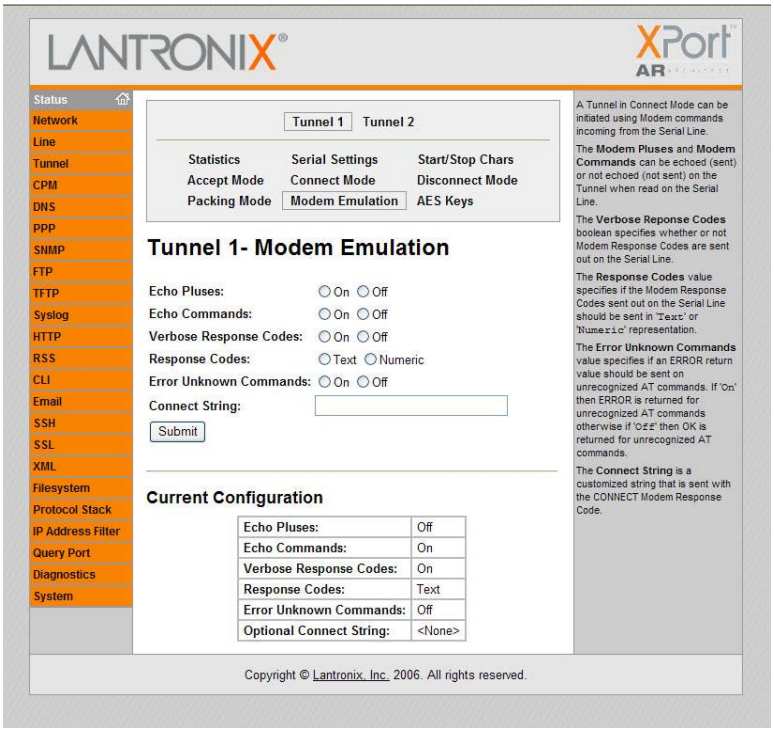
Modem Emulation

Configure the modem emulation settings when selecting Modem Emulation as the Tunnel 1 or Tunnel 2 Connect Mode type.

To configure modem emulation:

1. Select **Tunnel 1 → Modem Emulation** from the navigation menu. The Tunnel 1 Modem Emulation window displays.

Figure 4-10. Tunnel 1 Modem Emulation



2. Enter or modify the following fields:

Echo Pluses	Select **On** to echo "+++" when entering modem command mode
Echo Commands	Select **On** to echo the modem commands to the console.
Verbose Response Codes	Select **On** to send modem response codes out on the serial line.
Response Codes	Select the type of response code from either **Text** or **Numeric**.
Connect String	Enter the **connect string**. This modem initialization string prepares the modem for communications. It is a customized string sent with the "CONNECT" modem response code.

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

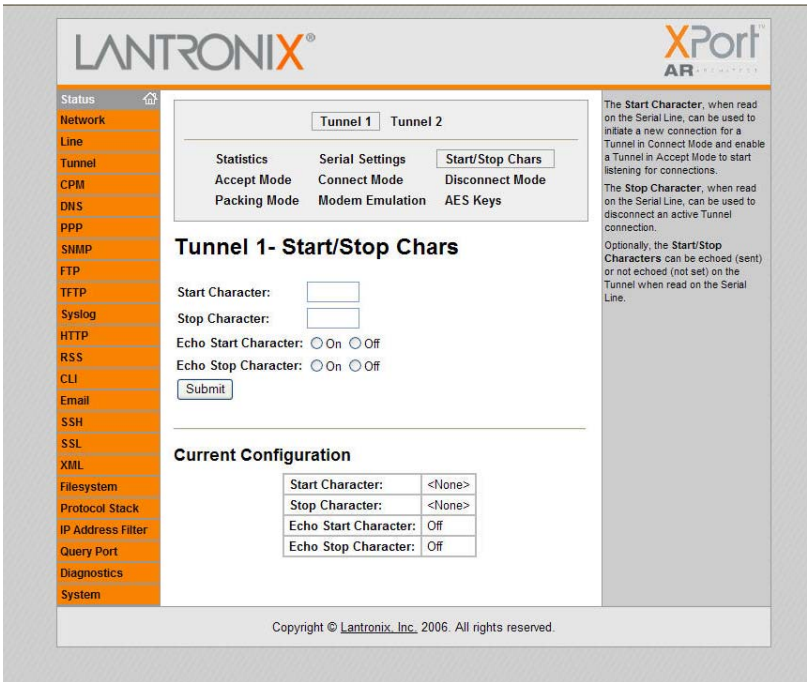
Start and Stop Characters

The XPort AR can be configured to start a tunnel when it receives a specific start character from the serial port. The XPort AR can also be configured to disconnect upon receiving the stop character.

To configure the start and stop characters mode:

1. Select **Tunnel 1 → Stop/Start Chars** from the navigation menu. The Tunnel 1 Start/Stop Chars window displays.

Figure 4-11. Tunnel 1 Start/Stop Chars



2. Enter or modify the following fields:

Start Character	Enter the start character in either ASCII or hexadecimal notation.
Stop Character	Enter the start character in either ASCII or hexadecimal notation.
Echo Start Character	Select **On** to forward (tunnel) the start character.
Echo Stop Character	Select **On** to forward (tunnel) the stop character.

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

Disconnect Mode

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

To configure the tunnel's disconnect mode:

1. Click **Tunnel 1** → **Disconnect Mode** from the navigation menu. The Tunnel 1 Disconnect Mode window displays.

Figure 4-12. Tunnel 1 Disconnect Mode

2. Enter or modify the following fields:

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

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

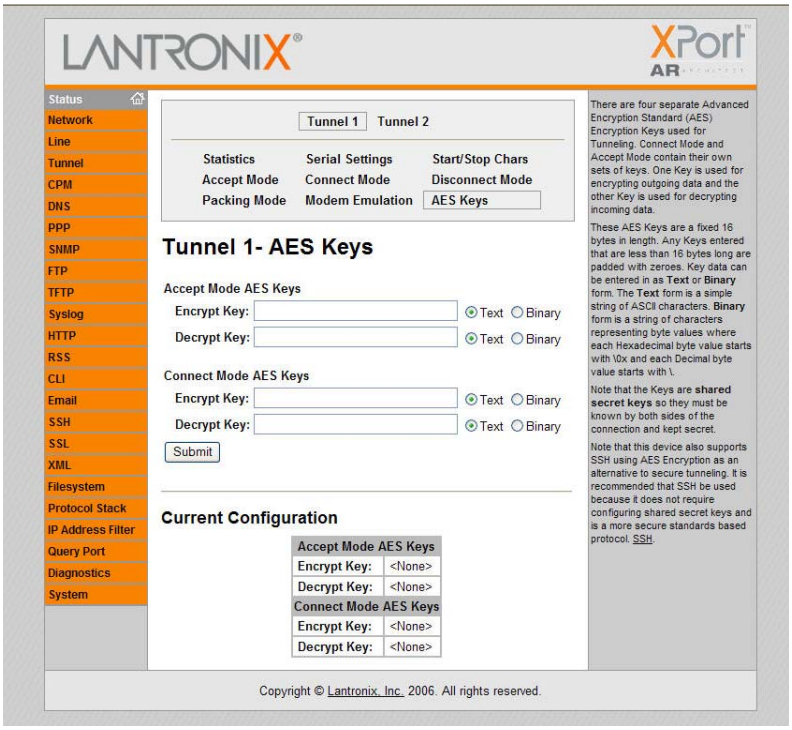
AES Keys – Connect Mode

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

To configure the AES keys for connect mode:

1. Click **Tunnel 1→ AES Keys – Connect** from the navigation menu. The Tunnel 1 AES Keys – Connect window displays.

Figure 4-13. AES Keys – Connect



2. Enter or modify the following fields:

Accept Mode AES Keys

Encrypt Key	Enter the value for each byte. From the pull-down menu, select the format for the byte as either character, hexadecimal, or decimal notation. ***Note:*** *Any empty trailing bites that are not specified are set to 0.*
Decrypt Key	Enter the value for each byte of the decrypt key. From the pull-down menu, select the format for the byte as either character, hexadecimal, or decimal notation. ***Note:*** *Any empty trailing bites that are not specified are set to 0.*

Connect Mode AES Keys

Encrypt Key	Enter the value for each byte. From the pull-down menu, select the format for the byte as either character, hexadecimal, or decimal notation. All trailing bytes not specified are set to 0.
Decrypt Key	Enter the value for each byte of the decrypt key. From the pull-down menu, select the format for the byte as either character, hexadecimal, or decimal notation. All trailing bytes not specified are set to 0.

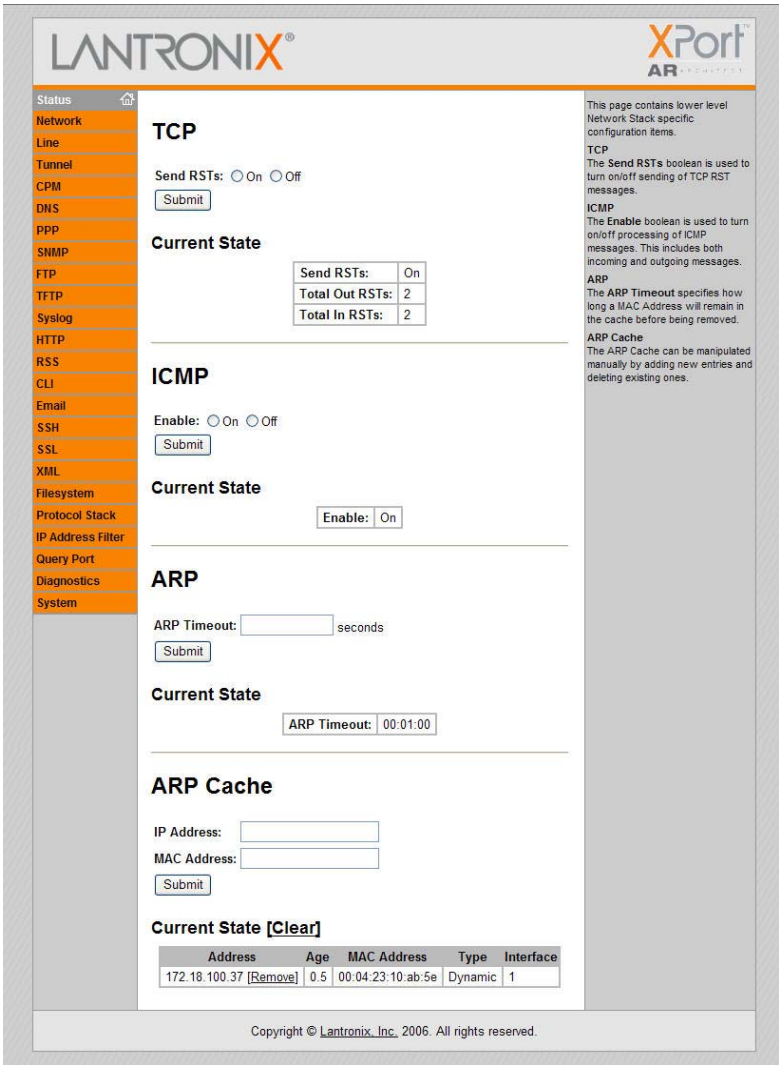
3. Click **Submit**. Changes are applied immediately to the XPort AR.

Protocol Stack Configuration

To configure the XPort AR's network stack protocols:

1. Click **Network → Protocol Stack** from the navigation menu. The Protocol Stack window displays the settings for TCP, ICMP, and ARP.

Figure 4-14. Protocol Stack



2. Enter or modify the following fields:

TCP

Send RSTs	TCP contains six control bits, with one or more defined in each packet. RST is one of the control bits. The RST bit is responsible for telling the receiving TCP stack to immediately end a connection. Sending this flag may pose a security risk. Select **Off** to disable the sending of the RST flag.

ICMP

Enable	*Internet Control Message Protocol (ICMP) can be used as an error-reporting protocol between two hosts. Commands such as ping use this protocol. Sending and processing ICMP messages may post a security risk.*

ARP

ARP Timeout	Enter the time, in milliseconds, for the ARP timeout. This is the duration an address remains in the cache.

ARP Cache

IP Address	Enter the IP address to add to the ARP table.
MAC Address	Enter the MAC address to add to the ARP table.

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

Current State

Clear	Select **Clear** to remove all entries in the ARP table.
Remove	Removes a specific entry from the ARP table.

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

Configurable Pin Manager

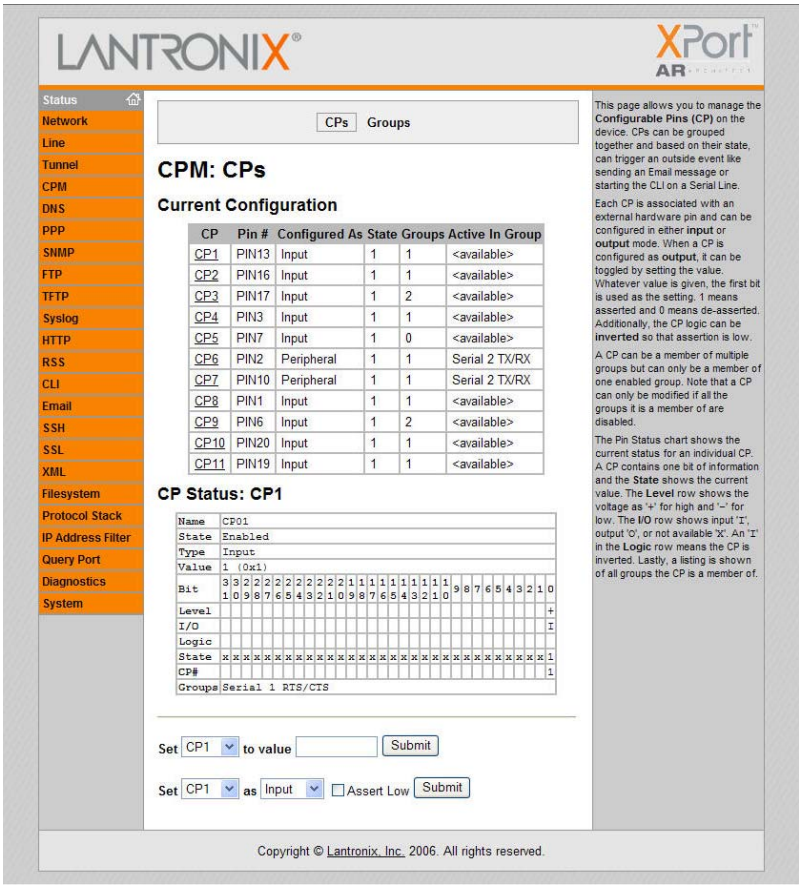
The XPort AR has 11 Configurable Pins (CPs). CPs can be grouped together using the Configurable Pin Manager (CPM). Each CP is associated to an external hardware pin. CPs can trigger an outside event (such as sending an email message or starting Command Mode).

CPM: Configurable Pins

To configure the XPort AR's CPs:

1. Click **CPM → CPs** from the navigation menu. The CPM: CPs window displays.

Figure 4-15. CPM: CPs



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

Current Configuration

CP	Indicates the Configurable Pin number.
Pin #	Indicates the hardware pin number associated with the CP.
Configured As	Displays the CPs configuration. A CP configured as **Input** is set to read input. A CP configured as **Output** drives data out of the XPort AR. **Peripheral** is a setting assigned by the XPort AR.
Binary	A value of **1** means asserted. **0** means de-asserted. **I** indicates the CP is inverted.
Groups	Indicates the number of groups in which the CP is a member.
Active In Group	A CP can be a member of several groups. However, it may only be active in one group. This field displays the group in which the CP is active.

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

CP Status

Name	Displays the CP number.
State	Current enable state of the CP. ***Note:*** *Peripheral pins are locked.*
Value	Displays the last bit in the CP's current value.
Bit	Visual display of the 32 bit placeholders for a CP.
I/O	A "+" symbol indicates the CP is asserted (the voltage is high). A "-" indicates the CP voltage is low.
Logic	An "I" indicates the CP is inverted.
Binary	Displays the assertion value of the corresponding bit.
CP#	Displays the CP number.
Groups	Lists the groups in which the CP is a member.

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

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

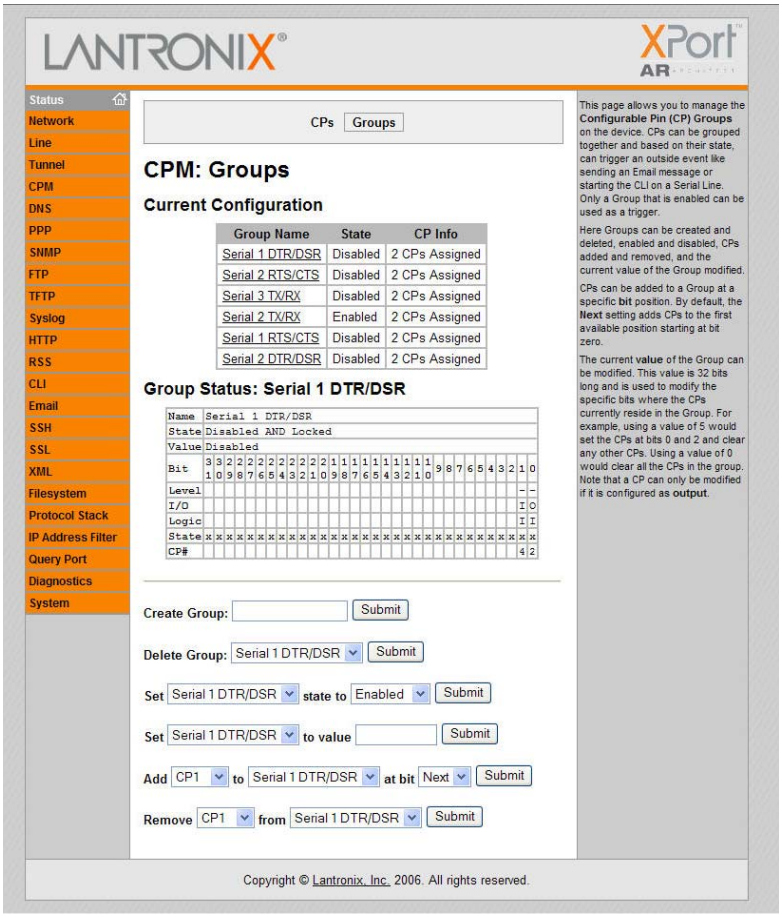
CPM: Groups

The CP Groups page allows for the management of CP groups. Create a CP group and add CPs to it. A group, based on its state, triggers outside events (such as sending email messages). Only an enabled group can be used as a trigger.

To configure the XPort AR's CP groups:

1. Click **CPM → Groups** from the navigation menu. The CPM: Groups window displays.

Figure 4-16. CPM: Groups



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

Current Configuration

Group Name	Displays the CP group's name.
State	Indicates whether the group is enabled or disabled.
CP Info	Provides CP group information.

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

Group Status

Name	Displays the CP Group name.
State	Current enable state of the CP group. ***Note:*** *Peripheral pins are locked.*
Value	Displays the CP group's current value.
Bit	Visual display of the 32 bit placeholders for a CP.
I/O	A "+" symbol indicates the CP's bit position is asserted (the voltage is high). A "-" indicates the CP voltage is low.
Logic	An "I" indicates the CP is inverted.
Binary	Displays the assertion value of the corresponding bit.
CP#	Displays the Configurable Pin number and its bit position in the CP group.

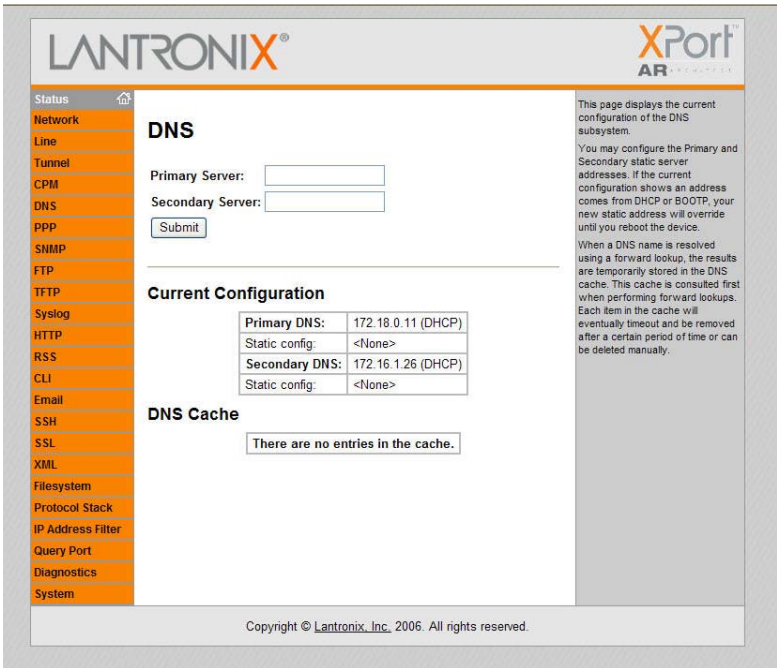
2. To create a CP group:
   a) Enter a group name in the **Create Group** field.
   b) Click **Submit**. Changes are applied immediately to the XPort AR.
3. To delete a CP group:
   a) Select the CP group from the **Delete Group** drop-down list.
   b) Click **Submit**. Changes are applied immediately to the XPort AR.
4. To enable or disable a CP group:
   a) Select the CP group from the **Set** drop-down list.
   b) Select the state (**Enabled** or **Disabled**) from the drop-down list.
   c) Click **Submit**. Changes are applied immediately to the XPort AR.
5. To set a CP group's value:
   a) Select the CP group from the **Set** drop-down list.
   b) Enter the CP group's value in the **value** field.
   c) Click **Submit**. Changes are applied immediately to the XPort AR.
6. To add CP to a CP group:
   a) Select the CP from the **Add** drop-down list.
   b) Select the CP group from the drop-down list.
   c) Select the CP's bit location from the **bit** drop-down menu.
   d) Click **Submit**. Changes are applied immediately to the XPort AR.
7. To delete a CP from a CP group:
   a) Select the CP from the **Remove** drop-down list.
   b) Select the CP group from the drop-down list.
   c) Click **Submit**. Changes are applied immediately to the XPort AR.

DNS Configuration

To configure the XPort AR's DNS configuration:

1. Click **Network → DNS** from the navigation menu. The DNS window displays.

Figure 4-17. DNS Settings



2. Enter or modify the following fields:

DNS

Primary Server	Enter the DNS primary server address.
Secondary Server	Enter the DNS secondary server address.

Current Configuration

Primary Server	Displays the current **Primary Server** address. Select **Delete** to remove this value.
Secondary Server	Displays the current **Secondary Server** address. Select **Delete** to remove this value.

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

PPP

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

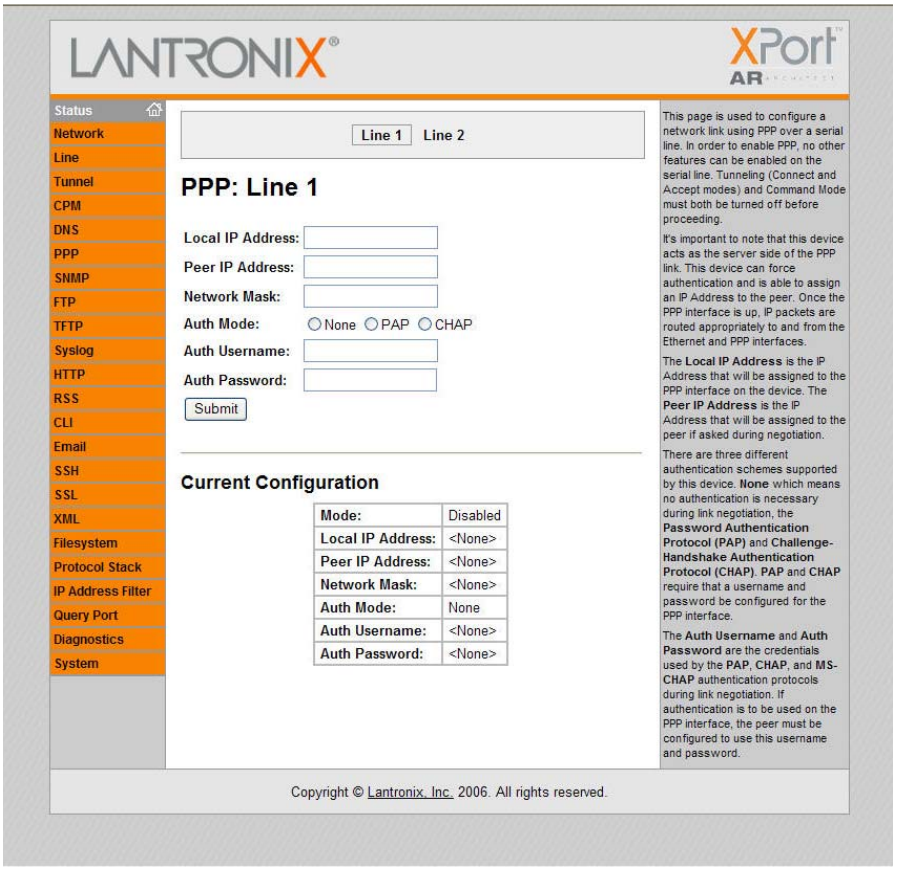
The XPort AR supports two types of PPP authorization: Password Authentication Protocol (PAP) and Challenge Handshake Protocol (CHAP). Both of these authentication methods require the configuration of a username and password. It also supports no authentication scheme when no authentication is required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

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

To configure the XPort AR's PPP configuration:

1. Click **Network → PPP Line 1** from the navigation menu. The PPP – Line 1 window displays.

Figure 4-18. PPP Settings



2. Enter or modify the following fields:

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).
Network Mask	Enter the network mask.
Auth. Mode	Choose the authentication mode. Select **None** when no authentication is required. Select **PAP** for Password Authentication Protocol. Select **CHAP** for the Challenge Handshake Authentication Protocol.

Auth. Username	Enter the username for use if authentication is used on the PPP interface.
Auth. Password	Enter the password for use if authentication is used on the PPP interface.

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

SNMP Configuration

To configure SNMP:

1. Click **Network → SNMP** from the navigation menu. The SNMP window opens and displays the current SNMP configuration.

Figure 4-19. SNMP Configuration

2. Enter or modify the following fields:

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

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

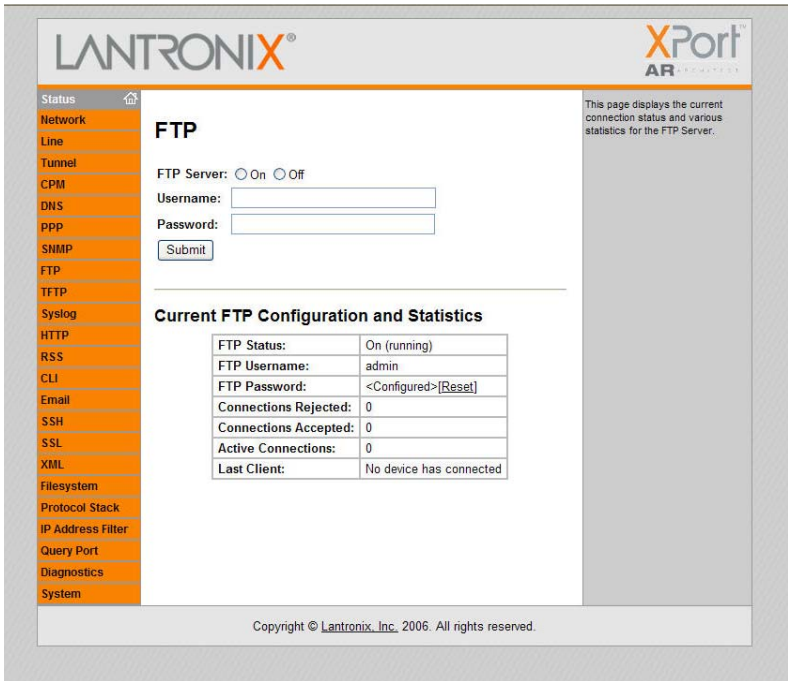
3. In the **Current Configuration** table, delete and clear currently stored fields as necessary.
4. Click **Submit**. Changes are applied immediately to the XPort AR.

FTP Configuration

To configure FTP:

1. Click **Network → FTP** from the navigation menu. The FTP window opens to display the current configuration.

Figure 4-20. FTP Configuration



2. Enter or modify the following fields:

FTP

FTP Server	Select **On** to enable the FTP server.
Username	Enter the username to use when logging in via FTP.
Password	Enter the password to use when logging in via FTP.

3. In the **Current FTP Configuration and Statistics** tables, reset currently stored fields as necessary by clicking the **Reset** link.

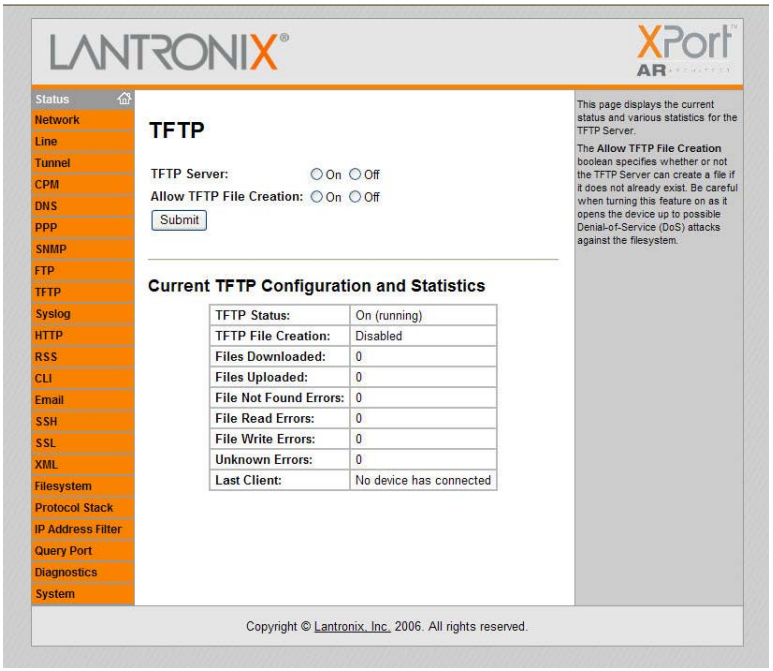
4. Click **Submit**. Changes are applied immediately to the XPort AR.

TFTP Configuration

To configure TFTP:

1. Click **Network → TFTP** from the navigation menu. The TFTP window opens to display the current configuration.

Figure 4-21. TFTP Configuration



2. Enter or modify the following fields:

TFTP

TFTP Server	Select **On** to enable the FTP server.
Allow TFTP File Creation	Enable the automatic creation of files stored by the TFTP server.

3. In the **Current TFTP Configuration and Statistics** table, reset currently stored fields as necessary by clicking the **Reset** link.

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

IP Address Filter

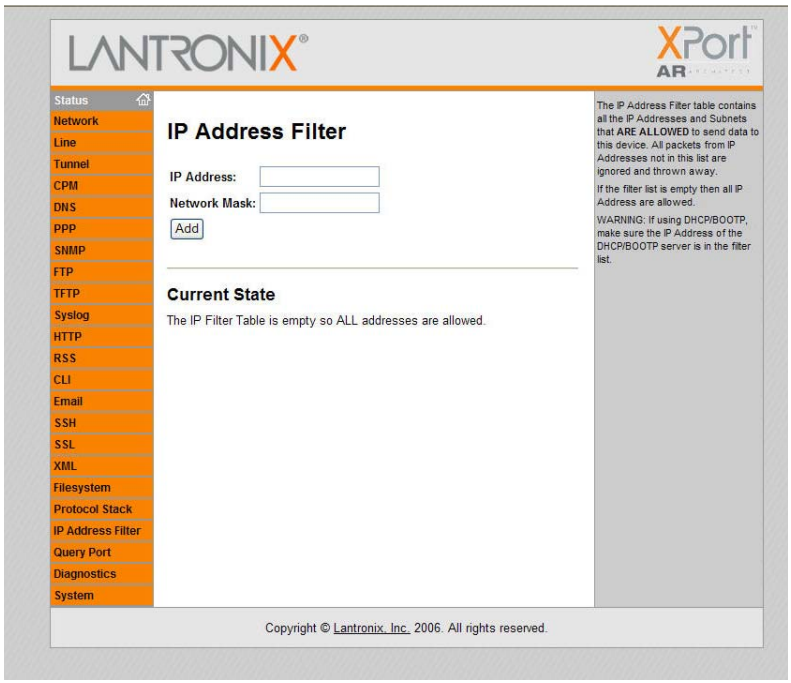
The IP address filter specifies the hosts and subnets permitted to communicate with the XPort AR.

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

To configure the IP address filter:

1. Click **Network → IP Address Filter** from the navigation menu. The IP Address Filter window opens to display the current configuration.

Figure 4-22. IP Address Filter Configuration



2. Enter or modify the following fields:

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

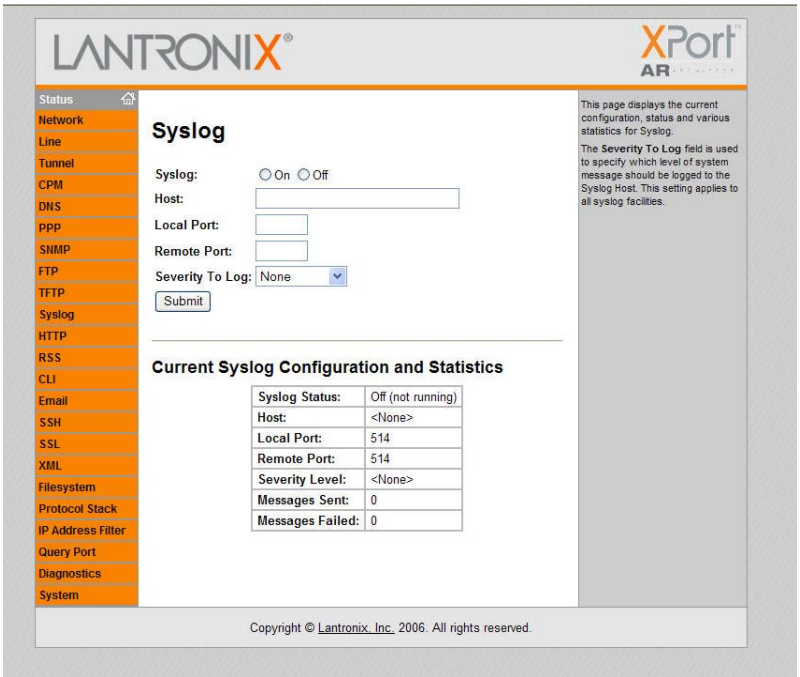
3. In the **Current State** table, click **Remove** to delete fields as necessary.
4. Click **Submit**. Changes are applied immediately to the XPort AR.

Syslog

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

1. Click **Syslog** from the navigation menu. The Syslog window opens to display the current configuration.

Figure 4-23. Syslog



2. Enter or modify the following fields:

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 EDS to which system logs are sent. The system log is always saved to local storage, but it is not retained through reboots. Saving the system log to a server that supports remote logging services (see RFC 3164) allows the administrator to save the complete system log history. The default is 514.
Remote Port	Enter the number of the port on the remote server that supports logging services. The default is 514.
Severity to Log	From the drop-down box, select the minimum level of system message the EDS should log. This setting applies to all syslog facilities. The drop-down list is in descending order of severity (e.g., Emergency is more severe than Alert.)

HTTP Settings

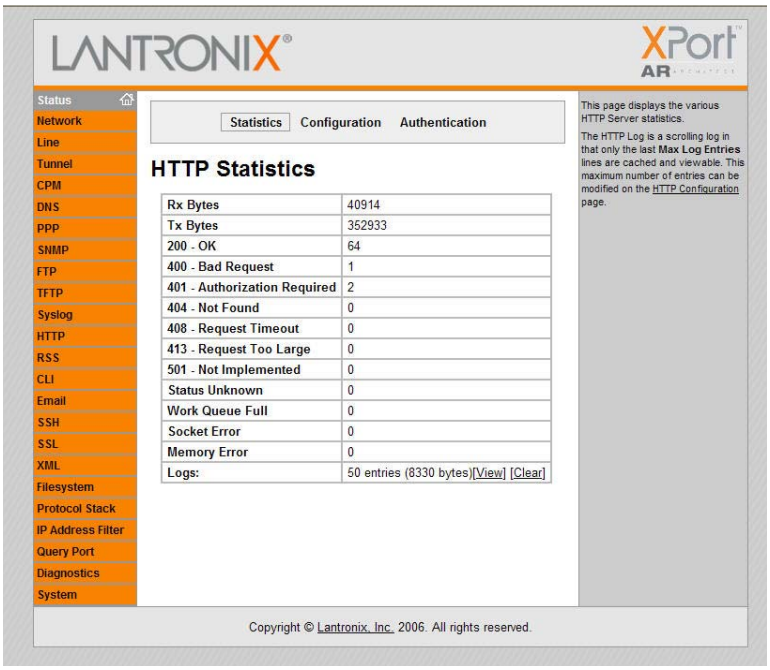
Hypertext Transfer Protocol (HTTP) is the transport protocol for communicating hypertext documents on the Internet. HTTP defines how messages are formatted and transmitted. It also defines the actions Web servers and browsers should take in response to different commands.

Select the **HTTP** link on the left menu bar to display the **HTTP** menu. The sub-menus allow for HTTP configuration, HTTP authentication administration, or RSS configuration.

To view HTTP statistics:

1. Click **HTTP → Statistics** from the navigation menu. The HTTP Statistics window displays.

Figure 4-24. HTTP Statistics



HTTP Configuration

To configure HTTP:

1. Click **HTTP → HTTP Configuration** from the navigation menu. The HTTP Configuration window opens.

Figure 4-25. HTTP Configuration

2. Enter or modify the following fields:

HTTP Server	Select **On** to enable the HTTP server.
HTTP Port	Enter the port for the HTTP server to use. The default is 80.
HTTPS Port	Enter the port for the HTTPS server to use. The default is 443. The HTTP server only listens on the **HTTPS Port** when an SSL certificate is configured.
Max Timeout	Enter the maximum time for the HTTP server to wait when receiving a request. This prevents Denial-of-Service (DoS) attacks. The default is 10 seconds.
Max Bytes	Enter the maximum number of bytes the HTTP server accepts when receiving a request. The default is 32 KB (this prevents DoS attacks).
Logging	Select **On** to enable HTTP server logging.
Max Log Entries	Sets the maximum number of HTTP server log entries. Only the last **Max Log Entries** are cached and viewable.
Log Format	Set the log format string for the HTTP server. The **Log Format** directives are as follows: **%a** - remote IP address (could be a proxy) **%b** - bytes sent excluding headers **%B** - bytes sent excluding headers (0 = '-') **%h** - remote host (same as '%a') **%{h}i** - header contents from request (h = header string) **%m** - request method

	%p - ephemeral local port value used for request **%q** - query string (prepend with '?' or empty '-') **%t** - timestamp HH:MM:SS (same as Apache '%(%H:%M:%S)t' or '%(%T)t') **%u** - remote user (could be bogus for 401 status) **%U** - URL path info **%r** - first line of request (same as '%m %U%q <version>') **%s** - return status

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

HTTP Authentication

To configure HTTP authentication settings:

1. Click **HTTP → Authentication** from the navigation menu. The HTTP Authentication window opens.

Figure 4-26. HTTP Authentication

2. Enter or modify the following fields:

URI	Enter the Uniform Resource Identifier (URI).
Realm	Enter the domain, or realm, used for HTTP. Required with the **URI** field.
Auth Type	Select the authentication type. **None** means no authentication is necessary. **Basic** encodes passwords using Base64. **Digest** encodes passwords using MD5. **SSL** means the page can only be accessed over SSL (no password is required). **SSL/Basic** means the page is accessible only over SSL and encodes passwords using Base64. **SSL/Digest** means the

	page is accessible only over SSL and encodes passwords using MD5.
Username	Enter the **Username** used to access the **URI**.
Password	Enter the **Password** for the **Username**.

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

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

Note: *More than one **Username** per **URI** is permitted. Click **Submit** and enter the next **Username** as necessary.*

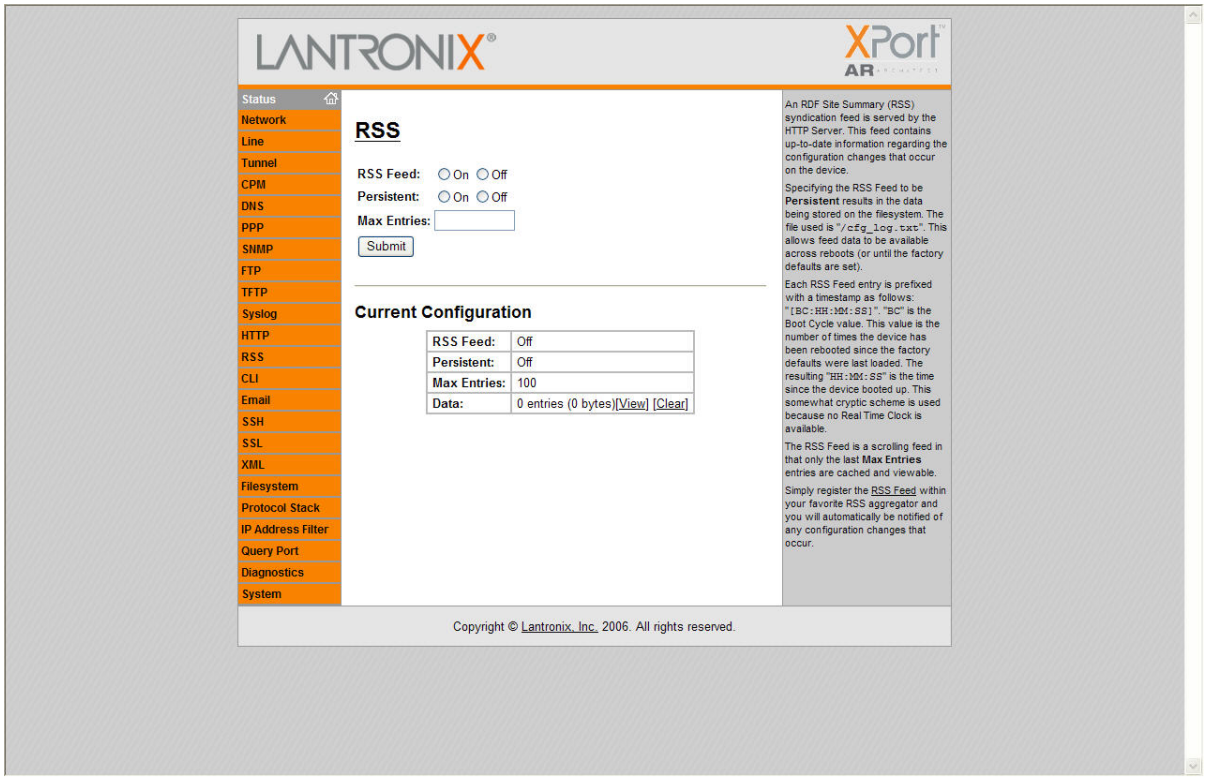
RSS

Rich Site Summary (RSS) 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 are also stored to the filesystem's cfg_log.txt file.

To configure RSS settings:

1. Click **RSS** from the navigation menu. The RSS window opens and displays the current RSS configuration.

Figure 4-27. RSS



2. Enter or modify the following fields:

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

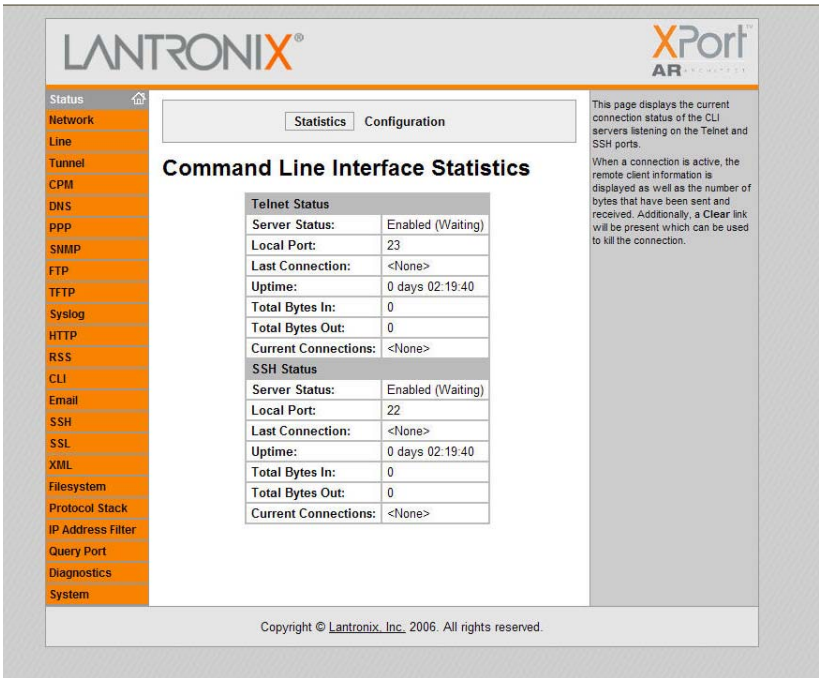
3. In the **Current Configuration** table, view and clear currently stored fields as necessary.

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

Command Line Interface Settings

Select the **CLI** link on the left menu bar to display the **Command Line Interface** menu.

Figure 4-28. Command Line Interface Statistics

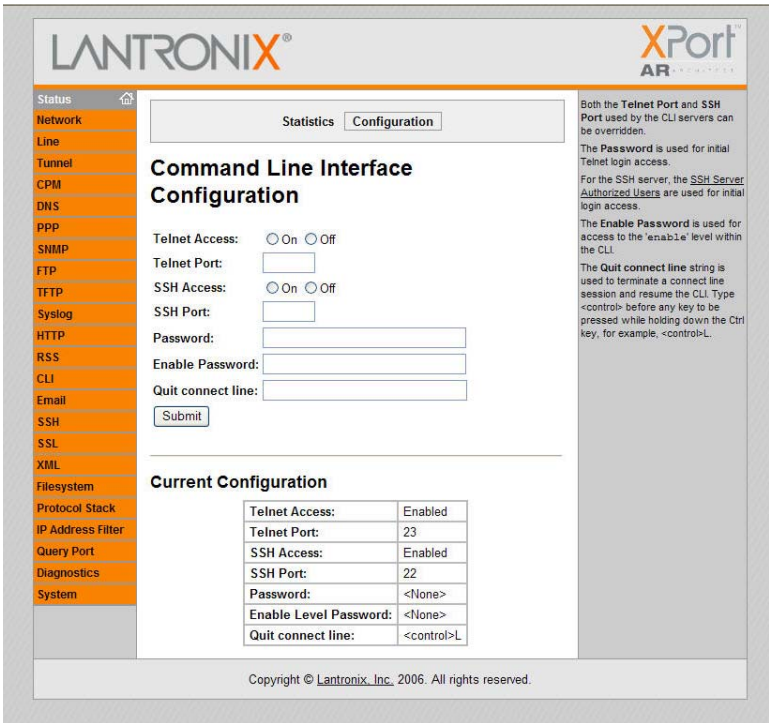


CLI Configuration

To configure the CLI:

1. Click **CLI** → **Configuration** from the navigation menu. The Command Line Interface window displays.

Figure 4-29. Command Line Interface Configuration



2. Enter or modify the following fields:

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

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

Email Configuration

The XPort AR allows for the configuration of four email alerts relating to the Configuration Pins (CPs). Select the **Email** link on the left menu bar to display the **Email** menu and statistics.

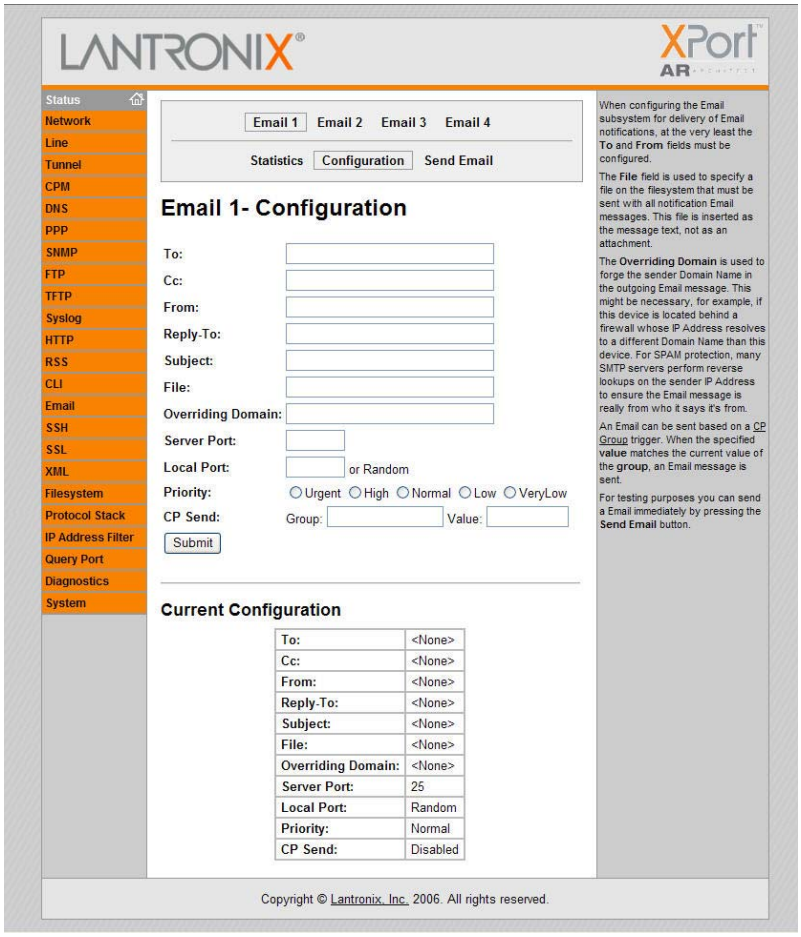
Note: *The following section describes the steps to configure **Email 1**; these steps also apply to **Email 2**, **Email 3**, and **Email 4** menu options.*

Figure 4-30. Email Statistics

To configure XPort AR's email settings:

1. Click **Email → Configuration** from the navigation menu. The Email Configuration window opens and displays the current Email configuration.

Figure 4-31. Email Configuration



2. Enter or modify the following fields:

To	Enter the email address to which the email alerts will be sent.
CC	Enter the email address to which the email alerts will be CCed.
From	Enter the email address to list in the From field of the email alert.
Reply-To	Enter the email address to list in the Reply-To field of the email alert.
Subject	Enter the subject for the email alert.
File	Enter the path of the file to send with the email alert. This file displays within the message body of the email.
Overriding Domain	Enter the domain name to override the current domain name in EHLO (Extended Hello).
Server Port	Enter the SMTP server port number. The default is a random port number.
Local Port	Enter the local port to use for email alerts.
Priority	Select the priority level for the email alert.

CP Send	Configure this field to send an email based on a CP Group trigger. An email is sent when the specified **Value** matches the current **Group**'s value.

3. In the **Current Configuration** table, delete currently stored fields as necessary.
4. Click **Submit**. Changes are applied immediately to the XPort AR.

SSH Settings

Secure Shell (SSH) is a protocol used to access a remote computer over an encrypted channel. It is a protocol for managing the security of data transmission over the Internet. It provides encryption, authentication, and message integrity services. Select the **SSH** link on the left menu bar to display the **SSH** menu over an encrypted channel. The sub-menus allow for the configuration of the SSH server (when the XPort AR acts as the server) and the SSH client (when the XPort AR acts as the client).

SSH Server's Host Keys

To configure the SSH server's host keys:

1. Click **SSH → Server Host Keys** from the navigation menu. The SSH Server: Host Keys window displays.

Figure 4-32. SSH Server: Host Keys

2. Enter or modify the following fields:

Host Keys

Private Key	Browse and locate the private key. Required when the **Public Key** is specified.
Public Key	Browse and locate the public key. Required when the **Private Key** is specified
Key Type	Select the key type. **DSA** is more secure than **RSA**. ***Note:*** *One set of RSA keys and one set of DSA keys are accepted.*

3. Click **Submit**. Changes are applied immediately to the XPort AR.
4. To create new keys, select the following option buttons:

Create New Keys

Key Type	Select **RSA** or **DSA**.
Bit Size	Select the size of the key. Large bit keys require more time to generate. ***Note:*** *Certain SSH clients require RSA host keys to be at least 1024 bits.*

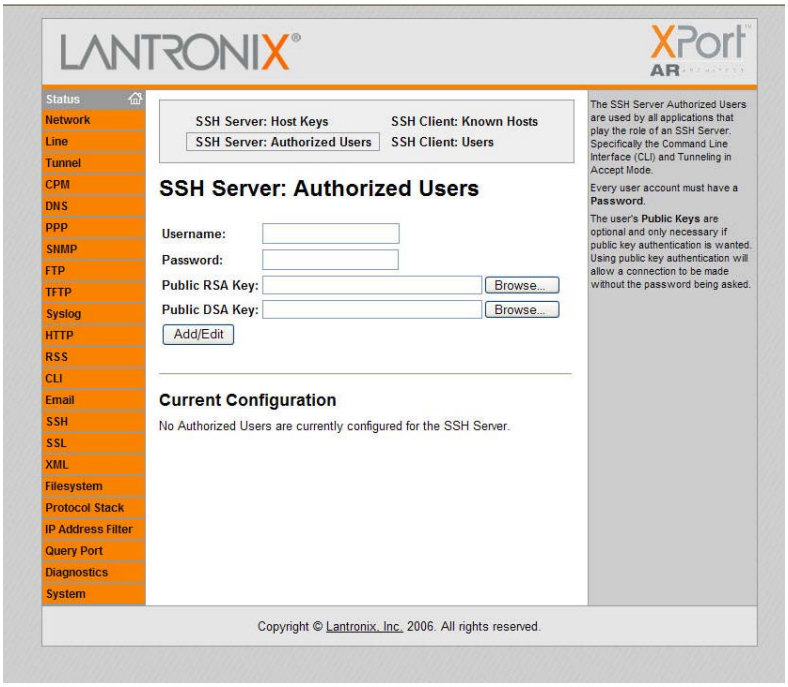
5. Click **Submit**. Changes are applied immediately to the XPort AR.

SSH Server's Authorized Users

To configure the SSH server's authorized users:

1. Click **SSH → Server Authorized Users** from the navigation menu. The SSH Server: Authorized Users window displays.

Figure 4-33. SSH Server: Authorized Users



2. Enter or modify the following fields:

Authorized Users

Username	Enter the username for an authorized user. Required when the **Password** is specified.
Password	Enter the password for SSH login to the XPort AR. Required when the **Username** is specified.
Public RSA Key	Browse and locate the RSA public key for this authorized user. This is used for key authentication. When successful, no password is requested.
Public DSA Key	Browse and locate the DSA public key for this authorized user. This is used for key authentication. When successful, no password is requested.

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

SSH Client Known Hosts

To configure the SSH client's known hosts:

1. Click **SSH → Client Known Hosts** from the navigation menu. The SSH Client: Known Hosts window displays.

Figure 4-34. SSH Client: Known Hosts

2. Enter or modify the following fields:

Server	Enter the hostname or IP address of the remote server location.
Public RSA Key	Click **Browse** to locate the public RSA key to use when authenticating the connection to the server.

Public DSA Key	Click **Browse** to locate the public DSA key to use when authenticating the connection to the server.

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

3. In the **Current Configuration** table, delete currently stored fields as necessary.
4. Click **Submit**. Changes are applied immediately to the XPort AR.

SSH Client User Configuration

To configure the SSH client's users:

1. Click **SSH → SSH Client Users** from the navigation menu. The SSH Client: Users window displays.

Figure 4-35. SSH Client: Users

2. Enter or modify the following fields:

Username	Enter the XPort AR's username for use when connecting to the server.
Password	Enter the password associated with the username.
Remote Command	Enter the remote command to provide to the server. This command triggers the desired or appropriate application to execute. A shell starts by default.
Private Key	Browse and locate the private key to use for authentication with the remote server.

Public Key	Browse and locate the public key to use for authentication with the remote server.
Key Type	Select the key type. **DSA** is more secure than **RSA**.

3. To create new keys, select the following option buttons:

Create New Keys

Key Type	Select **RSA** or **DSA**.
Bit Size	Select the size of the key. ***Note:*** *Large bit keys require more time to generate.*

4. Click **Submit**. Changes are applied immediately to the XPort AR.
5. In the **Current Configuration** table, delete currently stored fields as necessary.
6. Click **Submit**. Changes are applied immediately to the XPort AR.

SSL Settings

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

Select the **SSL** link on the left menu bar to display the **SSL** menu. The Web Manager also permits the creation of self-signed certificates. This type of SSL certificate is a certificate not signed by a valid Certificate Authority (CA).

To configure the XPort AR's SSL settings:

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

Figure 4-36. SSL

2. Enter or modify the following fields:

Upload Certificate

New Certificate	Browse and locate the digital certificate for use in SSL communications. Required field when configuring the **Private Key**.
New Private Key	Browse and locate the private key. This private key is a secret and known only to the certificate's owner. Required field when configuring a **New Certificate**.

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

4. To create a new self-signed certificate, enter the following information:

Create New Self-Signed Certificate

Country	Enter the 2-letter country code.
State/Province	Enter the state or province within the country.
Locality	Enter the city within the **State/Province**.
Organization	The name of the organization owning the certificate.
Organization Unit	The organization's division (unit) using the certificate.
Contact Name	Enter the Contact Name for the certificate.
Expires	Enter, in mm/dd/yyy format, the certificate's expiry date.
Bit Size	Select the certificate's bit size. ***Note:*** *Large bit keys require more time to generate.*

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

XML Configuration

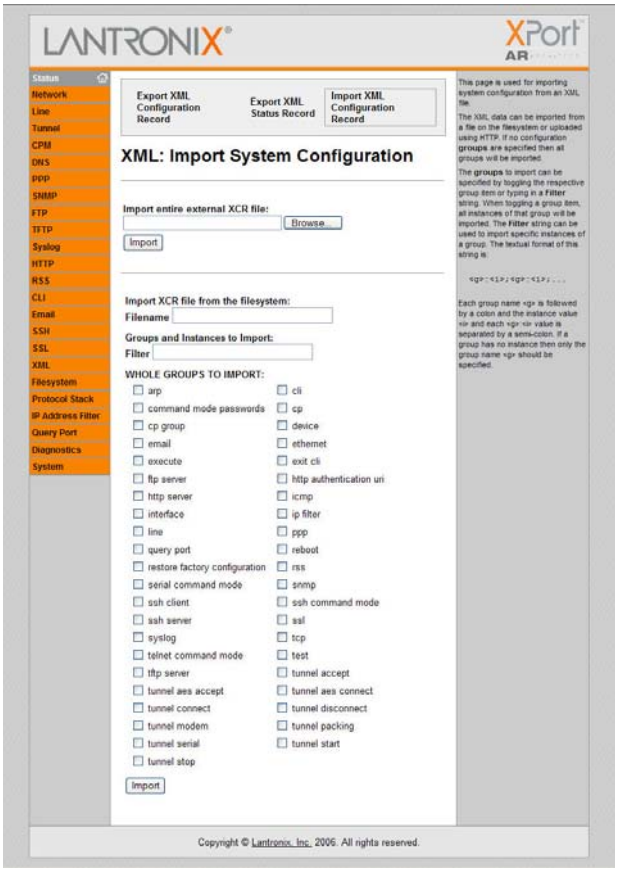
The XPort AR allows for the configuration of units using an XML configuration file. Export a current configuration for use on other XPort ARs or import a saved configuration file. For more information on using XML, see *XML* on page 92.

Import System Configuration

To import and apply an XML configuration:

1. Click **XML** → **Import** from the navigation menu. The XML: Import System Configuration window opens.

Figure 4-37. Import System Configuration



2. Use one of the following methods to import the XCR file:

   a) To import an external file, select **Import entire external XCR file** and click **Browse**. Locate the file in the Choose File window.

   b) To import an XCR file from the filesystem, select **Import XCR file from the filesystem** and enter the filename on the XPort AR containing the file to import.

3. (Optional) Enter the filter to apply in the **Filter** field. This selects the groups to import. The format of the input is:

   ```
   <g>:<i>;<g>:<i>; …
   ```

   Each group name (<g>) is followed by a colon (:) and the instance value (<i>). Each set of these ends with a semi-colon (;). If a group has no instance, specify only the group name (<g>).

4. Select from the list of checkboxes the groups to import. If no groups are selected, all the groups will be imported.

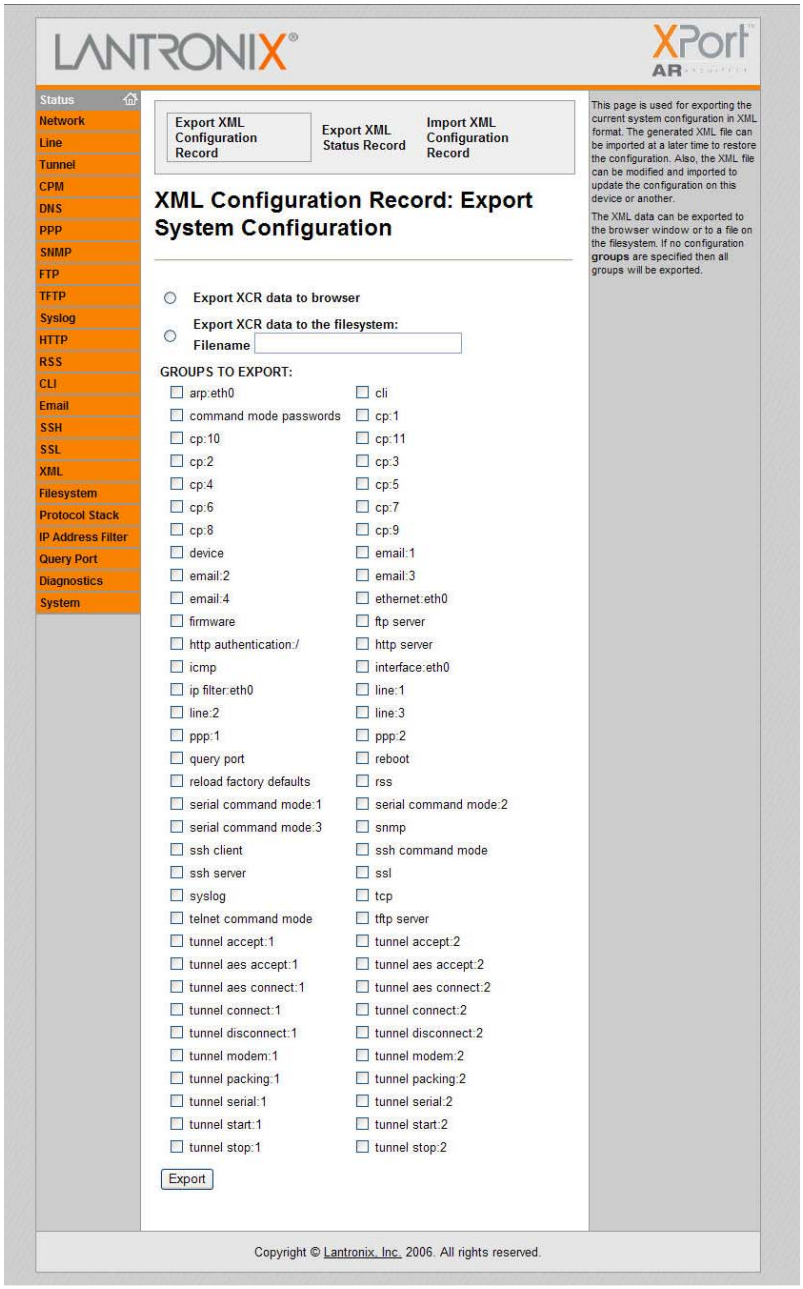
5. Click **Import**. The settings for the groups selected are applied to the XPort AR.

Export System Configuration

To export and store an XPort AR's configuration:

1. Click **XML → Export** from the navigation menu. The XML: Export System Configuration window opens.

Figure 4-38. Export System Configuration



2. Use one of the following methods to export the XCR file:

   a) To view the XCR data (without storing it), select **Export ECR data to browser**.

   b) To export to a file on the XPort AR filesystem, select **Export XCR data to the filesystem**. In the text box, enter the name for the file. The system will create the file and store it in the root directory of the XPort AR.

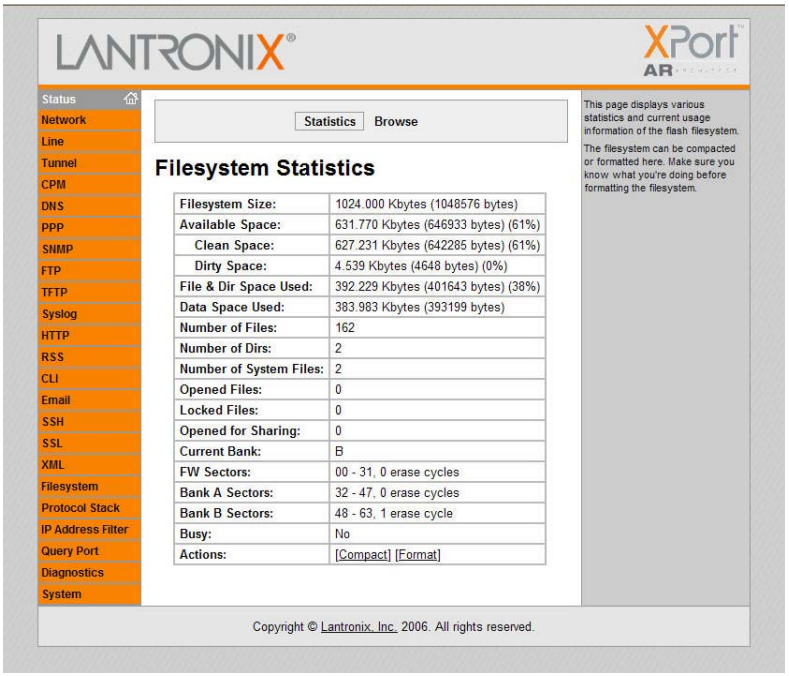
3. Select from the list of checkboxes the groups to export. By default, all groups are selected except those that affect network settings.

4. Click Export. The groups display if exporting the data to the browser. If exporting to the filesystem, the files are stored on the filesystem. (To view these files or store them elsewhere, see *Filesystem Configuration* on page 64.)

Filesystem Configuration

The XPort AR uses a flash filesystem to store files. Use the Filesystem option to view current file diagnostics or modify files.

Figure 4-39. Filesystem



To compact or format the XPort AR's filesystem:

1. Click **Filesystem** from the navigation menu. The Filesystem window opens and displays the current filesystem statistics and usage.

2. To compact the files, click **Compact**.

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

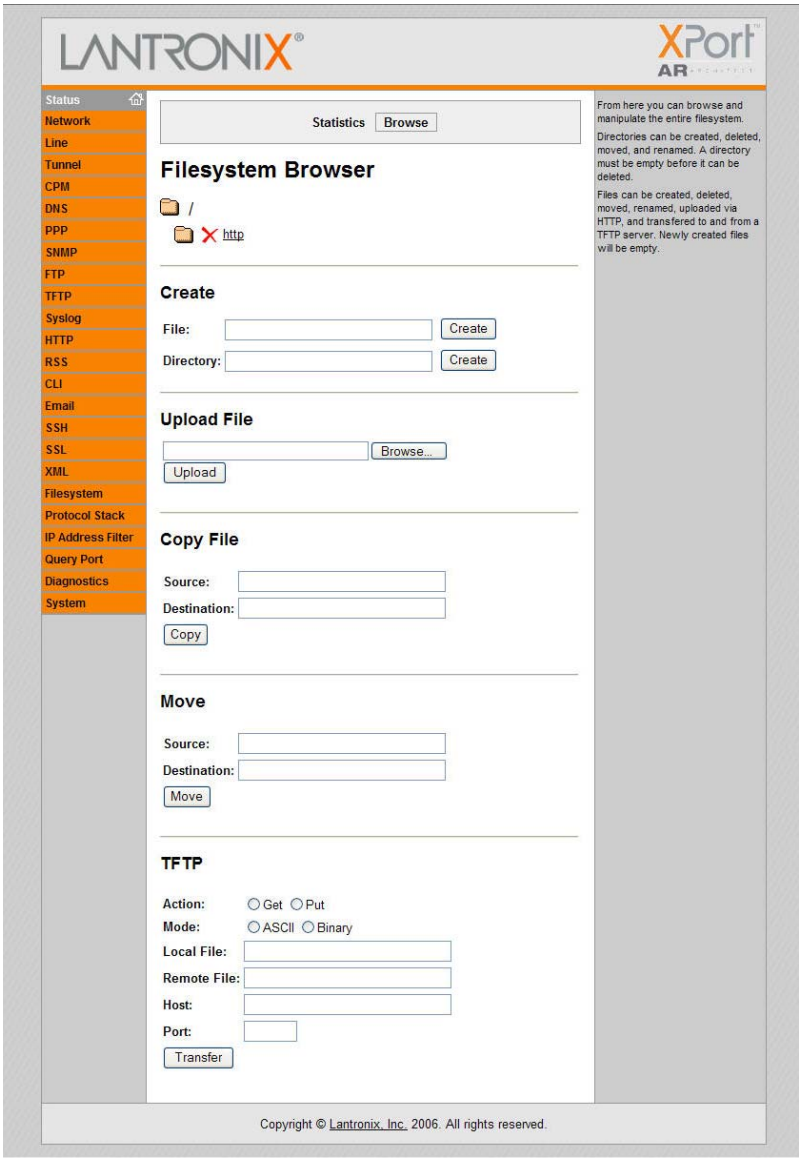
3. To reformat the filesystem, click **Format**.

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

To browse the XPort AR's filesystem:

1. Click **Filesystem → Browse** from the navigation menu. The Filesystem Browser window opens and displays the current filesystem configuration.

Figure 4-40. Filesystem Browser



2. Click on a filename to view the contents.

3. Click the **X** next to a filename to delete the file or directory. A directory can only be deleted if it is empty.

4. Enter or modify the following fields:

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

Create

File	Enter a filename and click **Create**. The XPort AR creates the empty file (0 bytes) and stores it in the current directory.
Directory	Enter a folder name and click **Create**. The XPort AR creates the folder and stores it in the current directory.

Upload File

Browse	Click **Browse** and locate the file to upload to the current filesystem directory. Click **Upload** to complete the process.

Copy File

Source	Enter the filename to copy.
Destination	Enter the folder where the **Source** file will be copied. Click **Copy** to complete the process. ***Note:*** *The* ***Source*** *and* ***Destination*** *filenames can be different.*

Move

Source	Enter the filename to move.
Destination	Enter the folder into which the **Source** file will be moved. Click **Move** to complete the process. ***Note:*** *When the* ***Source*** *and* ***Destination*** *filenames are different, the file and folder are renamed.*

TFTP

Action	Select **Get** or **Put**. Choose **Get** to receive a file. Choose **Put** to send a file.
Mode	Select **ASCII** or **Binary**.
Local File	Enter the name of the file to send to the remote location (**Put**) or to store locally (**Get**).
Remote File	Enter the name of the file on the remote location to store externally (**Put**) or to store locally (**Get**).
Host	Enter the IP address or hostname of the remote location.
Port	Enter the port number for TFTP communication. Click **Transfer** to complete the file transfer. The default is port 69.

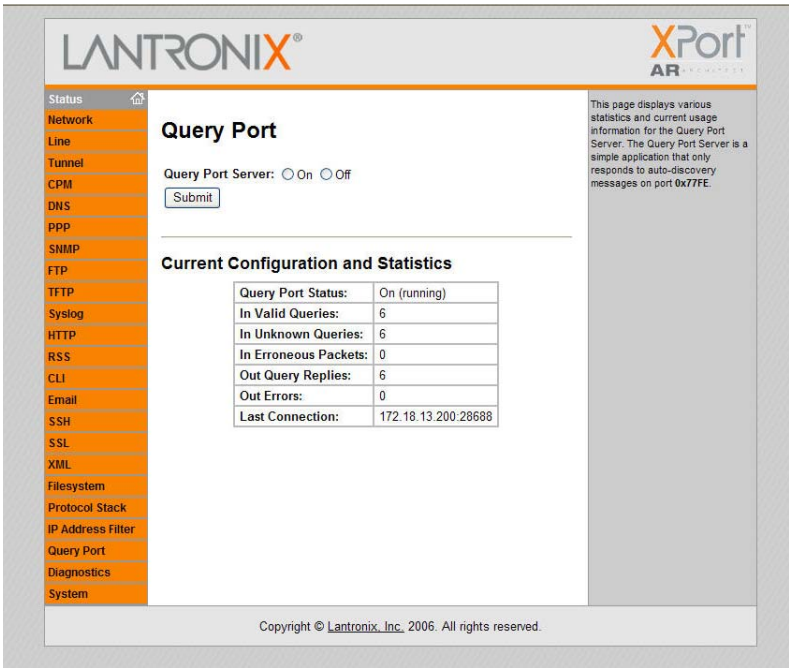
Query Port

The query port (0x77FE) is used for the automatic discovery of the device by the DeviceInstaller utility. Only 0x77FE discover messages from DeviceInstaller are supported. For more information on DeviceInstaller, see *Using DeviceInstaller* on page 16.

To configure the query port server:

1. Click **Network → Query Port** from the navigation menu. The Query Port window opens to display the current configuration.

Figure 4-41. Query Port Configuration



2. Select **On** to enable the query port server.
3. Click **Submit**. Changes are applied immediately to the XPort AR.

Diagnostics Configuration

The XPort AR has several tools for diagnostics and statistics. Select the **Diagnostics** link on the left menu bar to display the **Diagnostics** menu. The sub-menus allow for the configuration or viewing of MIB2 statistics, IP socket information, ping, traceroute, DNS lookup, memory, buffer pools, processes, and hardware.

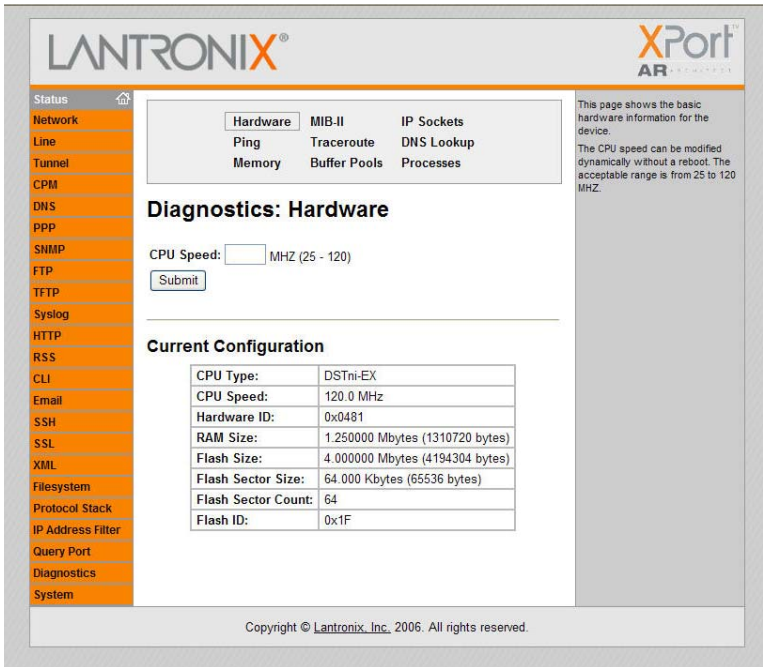
Hardware

The Hardware window displays basic hardware information and allows for the modification of the CPU speed.

To display the XPort AR's hardware diagnostics:

1. Click **Diagnostics → Hardware** from the navigation menu. The Diagnostics: Hardware window opens and displays current the current hardware configuration.

Figure 4-42. Diagnostics: Hardware



2. Enter or modify the following field:

CPU Speed	Enter the XPort AR's CPU speed. Accepted values are between 25 and 120 MHz.

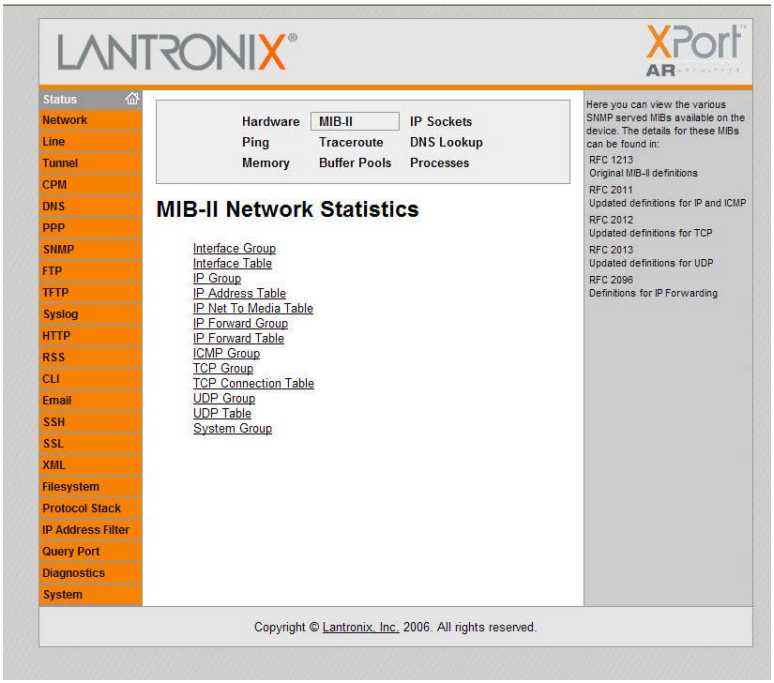
3. Click **Submit**. The CPU speed is updated immediately (no reboot required).

MIB-II Statistics

To view XPort AR's MIB-II statistics:

1. Click **Diagnostics → MIB-II Statistics** from the navigation menu. The MIB2 Network Statistics window opens.

Figure 4-43. MIB-II Network Statistics



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

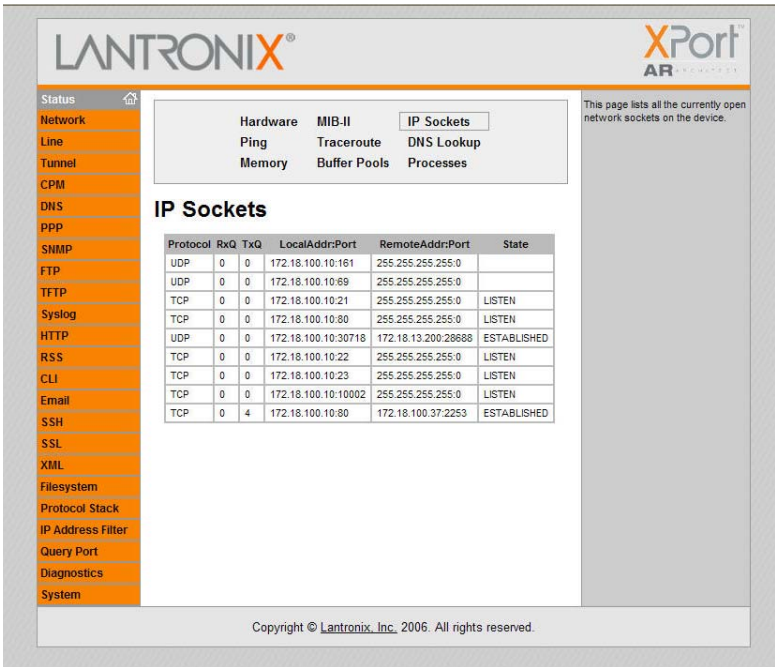
RFC 1213	Original MIB2 definitions.
RFC 2011	Updated definitions for IP and ICMP.
RFC 2012	Updated definitions for TCP.
RFC 2013	Updated definitions for UDP.
RFC 2096	Definitions for IP forwarding.

IP Sockets

To display open network sockets on the XPort AR:

1. Click **Diagnostics → IP Sockets** from the navigation menu. The IP Sockets window opens and displays all of the open network sockets on the XPort AR.

Figure 4-44. IP Sockets



Ping

To ping a remote device or computer:

2. Click **Diagnostics → Ping** from the navigation menu. The Diagnostics: Ping window opens.

Figure 4-45. Diagnostics: Ping

3. Enter or modify the following fields:

Host	Enter the IP address for the XPort AR to ping.
Count	Enter the number of ping packets XPort AR should attempt to send to the **Host**. The default is 3.
Timeout	Enter the time, in seconds, for the XPort AR to wait for a response from the host before timing out. The default is 5 seconds.

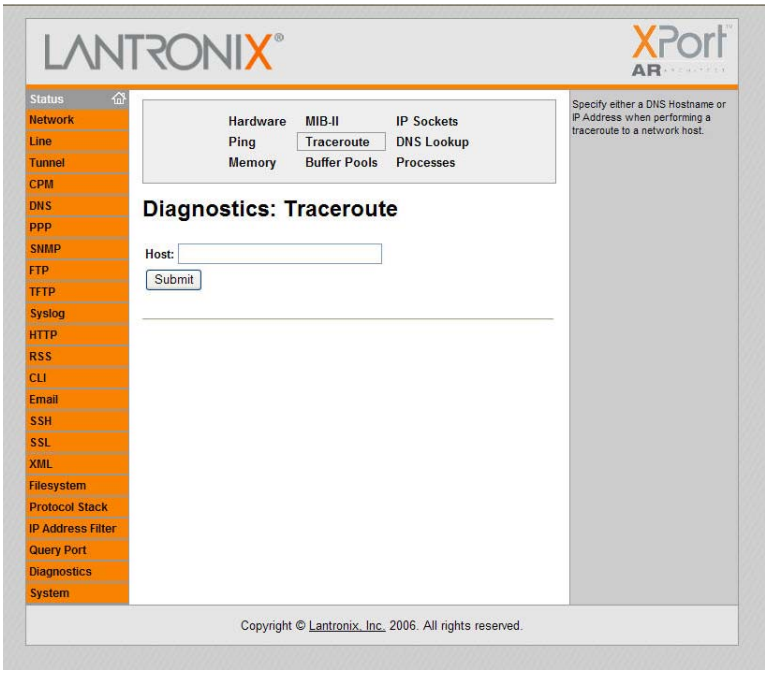
4. Click **Submit**. The results of the ping display in the window.

Traceroute

To use traceroute from the XPort AR:

1. Click **Diagnostics → Traceroute** from the navigation menu. The Diagnostics: Traceroute window opens.

Figure 4-46. Diagnostics: Traceroute



2. Enter or modify the following fields:

Traceroute	Enter the IP address or DNS hostname. This address is used to show the path between it and the XPort AR when issuing the traceroute command.

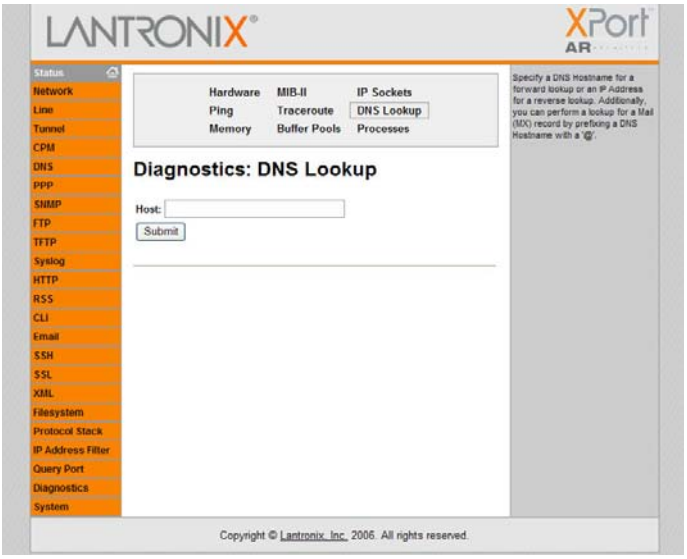
3. Click **Submit**. The results of the traceroute display in the window.

DNS Lookup

To use forward or reverse DNS lookup:

1. Click **Diagnostics → DNS Lookup** from the navigation menu. The Diagnostics: DNS Lookup window opens.

Figure 4-47. Diagnostics: DNS Lookup



2. Enter or modify the following field:

Host	Enter an IP address for reverse lookup to locate the hostname for that IP address. Enter a hostname for forward lookup to locate the corresponding IP address. Enter a domain name (prefixed with "@") to look up the Mail Exchange (MX) record IP address.

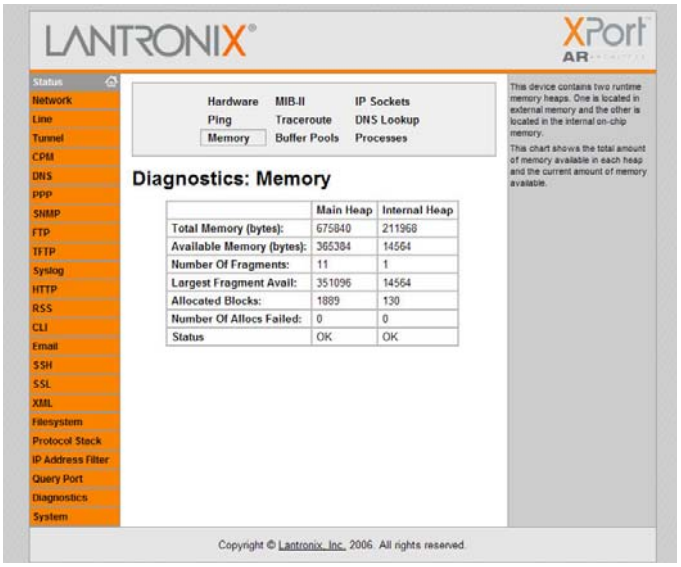
3. Click **Submit**. The results of the lookup display in the window.

Memory

To display memory statistics for the XPort AR:

1. Click **Diagnostics → Memory** from the navigation menu. The Diagnostics: Memory window displays.

Figure 4-48. Diagnostics: Memory



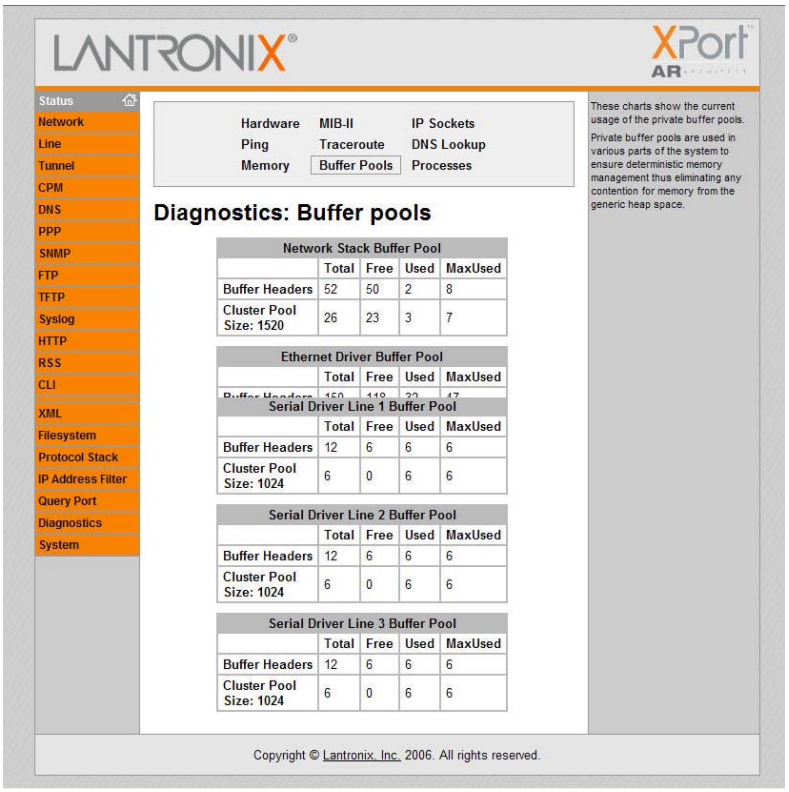
Buffer Pools

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

To display the XPort AR's buffer pools:

1. Click **Diagnostics → Buffer Pools** from the navigation menu. The Diagnostics: Buffer Pools window opens.

Figure 4-49. Diagnostics: Buffer Pools



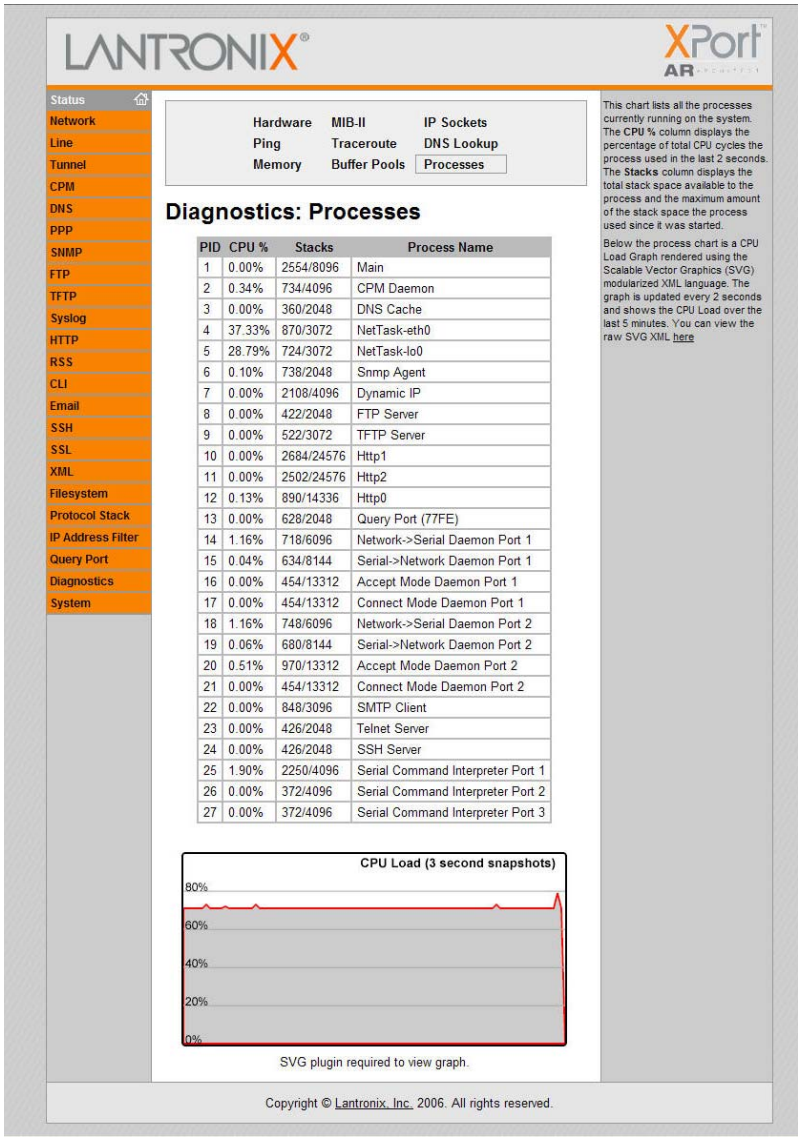
Processes

The XPort AR Processes window displays all the processes currently running on the system. It displays the Process ID (PID), the percentage of total CPU cycles a process used within the last 2 seconds, the total stack space available, the maximum amount of stack space used by the process since it started, and the process name.

To display the processes running on the XPort AR and their associated statistics:

1. Click **Diagnostics → Processes** from the navigation menu. The Diagnostics: Processes window opens.

Figure 4-50. Diagnostics: Processes

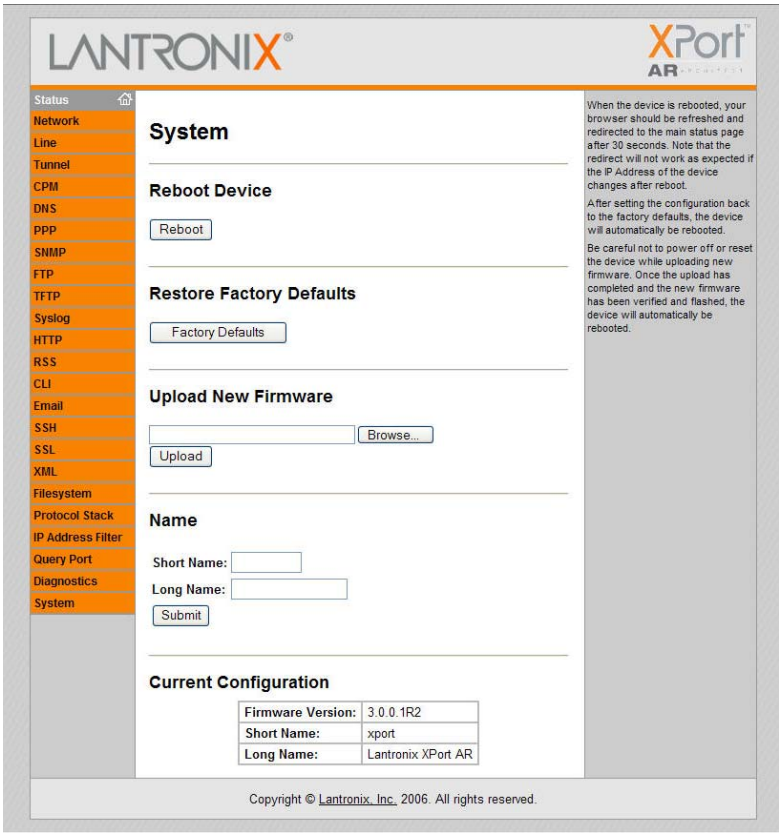


Note: *The Adobe SVG plug-in is required to view the CPU Load Graph.*

System Configuration

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

Figure 4-51. System



To configure the XPort AR's system settings:

1. Click **System** from the navigation menu. The System window opens.
2. Configure the XPort AR's system using the following fields:

Reboot Device	Click **Reboot** to reboot the XPort AR. The system refreshes and redirects the browser to the XPort AR's home page.
Restore Factory Defaults	Click **Factory Defaults** to restore the XPort AR to the original factory settings. All configurations will be lost. The XPort AR automatically reboots upon setting back to the defaults.
Upload New Firmware	Click **Browse** to locate the firmware file location. Click **Upload** to install the firmware on the XPort AR. The device automatically reboots upon the installation of new firmware.
Name	Enter a new **Short Name** and a **Long Name** (if necessary). The **Short Name** is a maximum of 8 characters. Changes take place upon the next reboot.

5: Point-to-Point Protocol (PPP)

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

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

PAP is an authentication protocol in PPP. It offers a straightforward method for the peer to determine its identity. Upon the link establishment, the user ID and password are repeatedly sent to the authenticator until it is acknowledged or the connection is terminated.

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

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

Note: *RFC1334 defines both CHAP and PAP.*

Use the XPort AR's Web Manager or CLI to configure a network link using PPP over a serial line. Turn off Connect Mode, Accept Mode, and Command mode before enabling PPP.

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

6: Tunneling

Serial tunneling allows for devices to communicate over a network, without the realization of other devices connecting between them. Tunneling parameters are configured using the Web Manager's *Tunnel 1 and Tunnel 2 Settings* (on page 24) or Command Mode's Tunnel Menu (see the XPort AR Command Reference for the full list of commands.)

The XPort AR supports 2 tunneling connections simultaneously per serial port. One of these connections is Connect Mode, the other connection is Accept Mode. The connections on one serial port are separate from those on the other serial port.

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

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

Connect Mode

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

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

Connect Mode supports the following protocols:

- TCP
- AES encryption over UDP
- AES encryption over TCP
- SSH (the XPort AR is the SSH client)
- UDP (available only in Connect Mode since it is a connectionless protocol).

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

For Connect Mode using UDP, if the remote address or port is not configured, then the XPort AR accepts packets from any device on the network. It will send packets to the last device that sent it packets. As a result, it is advised to configure the remote address and port. When the remote port and station are configured, the XPort AR ignores date from other sources.

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

To ignore data sent to the XPort AR, enable the blocking of serial data or network data (or both).

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

To configure SSH, the SSH client username must be configured. In Connect Mode, the XPort AR is the SSH client. Ensure the XPort AR's SSH client username is configured on the SSH server before using it with the XPort AR.

Connect Mode has five states:

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

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

Configure the Modem Control Active setting (for DSR or DTR) to start a Connect Mode connection when the signal is asserted. The XPort AR will indefinitely try to make a connection forever. If the connection closes, it will not make another connection unless the signal is asserted again.

Accept Mode

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

Accept Mode supports the following protocols:

- SSH (the 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.
- TCP
- AES encryption over TCP

- Telnet/IAC mode (The XPort AR currently 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 (close the connection)
- Enabled (always listening for a connection)
- Active if it receives any character from the serial port
- Active if it receives a specific (configurable) character from the serial port (same start character as Connect Mode's start character)
- Modem control signal

Disconnect Mode

Disconnect Mode ends Accept Mode and Connect Mode connections. When disconnecting, the XPort AR shuts down connections gracefully.

The following 3 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.

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

Packing Mode

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

The following settings are configurable for Packing Mode:

- Disable Packing Mode
- The Packing Mode timeout. The data is packed for a specified period of time before being sent out.
- The Packing Mode threshold. When the buffer fills to a specified amount of data (and the timeout has not elapsed), the XPort AR packs the data and sends it out.
- The send character. Similar to a start or stop character, the XPort AR packs the data until it sees the send character. The XPort AR then sends the packed data and the send character in the packet.
- A trailing character. If a trailing character is defined, this character is appended to data put on the network immediately following the send character.

Modem Emulation

The XPort AR supports Modem Emulation mode for devices that send out modem signals. There are two different modes supported:

Command Mode: sends back verbal response codes.

Data Mode: information transferred in is also transferred out.

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

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

Command Mode

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

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

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

All of these commands behave like a modem. For commands that are valid but not applicable to the 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.

Note: Configure either the IP address using the address on its own (<xxx.xxx.xxx.xxx>), or the IP address and port number by entering <xxx.xxx.xxx.xxx>:<port> . The port number cannot be entered on its own.

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

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

By default, the +++ characters are not passed through the connection. Turn on this capability using the **modem echo plus** command.

Serial Line Settings

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

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

Statistics

The XPort AR logs statistics for tunneling. The **Dropped** statistic displays connections ended by the remote location. The **Disconnected** statistic displays connections ended by the XPort AR.

7: SSH and SSL Security

The XPort AR supports Secure Shell (SSH) and Secure Sockets Layer (SSL). These security protocols are configurable through the Web Manager (see *SSH Settings* on page 56 and *SSL Settings* on page 60) and Command Mode (see the XPort AR Command Reference for available SSH and SLL commands).

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

Secure Shell: SSH

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

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

SSH Server Configuration

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

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

To configure SSH server settings:

1. Click **SSH → Server Host Keys** from the navigation menu. The SSH Server: Host Keys page displays.
2. To configure the host keys:
   a) If the keys exist, locate the **Private Key** and **Public Key** using the **Browse** button. Select the **Key Type** (**RSA** is more secure) and click **Submit** to upload the keys.
      i. SSH keys may be created on another computer and uploaded to the XPort AR. To do so, use the following command using Open SSH to care a 768-bit DSA key pair:

```
ssh-keygen –b 768 –t dsa
```

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

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

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

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

SSH Client Configuration

To configure the XPort AR as an SSH client, there is one requirement:

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

To configure SSH client settings:

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

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

Secure Sockets Layer: SSL

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

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

On the XPort AR, configure an SSL certificate for the HTTP server to listen on the HTTPS port. This certificate can be created elsewhere and uploaded to the device.

Alternatively, it can be automatically generated on the device; this certificate type is a self-signed certificate.

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

To upload a new certificate, see *Upload Certificate* on page 61. To create a new self-signed certificate, see *Create New Self-Signed Certificate* on page 61.

8: Using Email

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

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

1. Via the Web Manager (See *Configuration Using Web Manager* on page 18).
2. Via Command Mode by using the Send command (See the XPort AR Command Reference for available email commands under the Chem Menu).
3. By configuring a CP or a CP group (See *Configuration Pin Manager* on page 89). When the CP or the CP group changes state to the pre-specified value, an email alert is sent.

SMTP Configuration

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

The minimum requirements for SMTP configuration are:

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

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

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

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

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

Priority Levels

The default priority level for the XPort AR's emails is Normal priority. The XPort AR has 5 configurable priority levels; certain recipient systems have filters based on these priority levels.

Configurable priority levels are:

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

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

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

DNS Records

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

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

Extended Hello

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

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

For a more information EHLO, see RFC 2821.

Email Statistics

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

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

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

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

9: Configuration Pin Manager

There are 11 configurable pins on the XPort AR. All CPs (except for 5) are shared by some other function on the XPort AR. Some of the CPs are assigned to serial port 1 (dtr/dsr for modem control and rts/cts for hardware flow control), others to serial port 2 (dtr/dsr for modem control, rts/cts for hardware flow control, and tx/rx groups as well).

CPs are configurable individually, or may be clustered together and configured as a single group (CP group). This increases flexibility when incorporating the XPort AR into another system.

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

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

Configurable Pins

To view a CP's configuration:

1. If using the Web Manager:
   a) Click **CPM → CPs** from the navigation menu. The CPM: Configurable Pin window displays.
   b) Click the specific **CP** from the Current Configuration table. The CP's configuration displays in the CP Status table.
2. If using Command Mode (the CLI):
   a) Enter Enable → CPM to access the CPM level menu.
   b) Type **show cp**.
3. The CP table displays the following:

CP	Indicates the Configurable Pin number.
Pin #	Indicates the hardware pin number associated with the CP.
Configured As	Displays the CPs configuration. A CP configured as **Input** is set to read input. A CP configured as **Output** drives data out of the XPort AR. **Peripheral** is a setting assigned by the XPort AR.

State	A value of **1** means asserted. **0** means de-asserted. **I** indicates the CP is inverted.
Groups	Indicates the number of groups in which the CP is a member.
Active In Group	A CP can be a member of several groups. However, it may only be active in one group. This field displays the group in which the CP is active.

CP Groups

To view a CP group's configuration:

1. If using the Web Manager:
   a) Click **CPM → Groups** from the navigation menu. The CPM: Groups window displays.
   b) Click the CP groups from the Current Configuration table. The CP's configuration displays in the Group Status table.
2. If using Command Mode (the CLI):
   a) Enter Enable → CPM to access the CPM level menu.
   b) Type **show group <name>**.
3. The Group Status table displays the following:

Name	Displays the CP number.
State	Current enable state of the CP. ***Note:*** *Peripheral pins are locked.*
Value	Displays the last bit in the CP's current value.
Bit	Visual display of the 32 bit placeholders for a CP.
I/O	A "+" symbol indicates the CP is asserted (the voltage is high). A "-" indicates the CP voltage is low.
Logic	An "I" indicates the CP is inverted.
Binary	Displays the assertion value of the corresponding bit.
CP#	Displays the CP number.
Groups	Lists the groups in which the CP is a member.

The CP group table displays the CPs assigned to it. It also displays the CP's bit position within the CP group. The wave form shows the actual voltage of inputs and outputs (a value of 1 indicates a high voltage). The state shows the assertion level.

To configure a group's value:

1. If using the Web Manager:
   a) Click **CPM → Groups** from the navigation menu. The CPM Groups window displays
   b) To create a CP group:

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

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

c) To delete a CP group:

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

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

d) To enable or disable a CP group:

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

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

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

e) To set a CP group's value:

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

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

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

f) To add CP to a CP group:

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

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

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

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

g) To delete a CP from a CP group:

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

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

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

2. If using Command Mode:

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

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

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

10: XML

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

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

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

11: Branding the XPort AR

The XPort AR's Web Manager and Command Mode (CLI) are customizable.

Web Manager Customization

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

Note: *To view these files, open the* ***http → config*** *folder using the Filesystem Browser. Alternatively, upload and download the files using FTP/TFTP. For more on the filesystem, see* *Filesystem Configuration on page 64.*

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

Command Mode

Customize the XPort AR's Command Mode by changing its short name and long name. The short name is used for show commands:

```
(enable)# show XPort
```

The long name appears in the Product Type field:

```
(enable)# show XPort
Product Information:
      Product Type: Lantronix XPort AR
```

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

1. Click **System** from the navigation menu. The System window opens.
1. In the **Short Name** field, enter the new short name for the device, up to 8 characters.
2. In the **Long Name** field, enter the new long name for the device.
3. Click **Submit**.
4. To apply changes, click **Reboot**.

12: Updating Firmware

Obtaining Firmware

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

Loading New Firmware

Reload the firmware using the XPort AR's Web Manager's System window.

To upload new firmware:

1. Click **System** from the navigation menu. The System window opens.
2. Click in the **Upload New Firmware** section, click **Browse**. A pop-up window displays; locate the firmware file.
3. Click **Upload** to install the firmware on the XPort AR. The device automatically reboots upon the installation of new firmware.

A: Technical Support

If you are experiencing an error that is not described in this user guide, or if you are unable to fix the error, you may:

- Check our online knowledge base at http://www.lantronix.com/support.
- Contact Technical Support in the US:

  Phone: 800-422-7044 (US only) or 949-453-7198

  Fax: 949-450-7226

  Our phone lines are open from 6:00AM - 5:30 PM Pacific Time Monday through Friday, excluding holidays.

- Contact Technical Support in Europe, Middle East, and Africa:

  Phone: +49 (0) 89 31787 817

  Email: eu_techsupp@lantronix.com

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

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

- Your name, and your company name, address, and phone number
- Lantronix model number
- Lantronix serial number
- Software version (on the first screen shown when you Telnet to port 9999)
- Description of the problem
- Debug report (stack dump), if applicable
- Status of the unit when the problem occurred (please try to include information on user and network activity at the time of the problem)

B: Binary to Hexadecimal Conversions

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

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

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

Converting Binary to Hexadecimal

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

Conversion Table

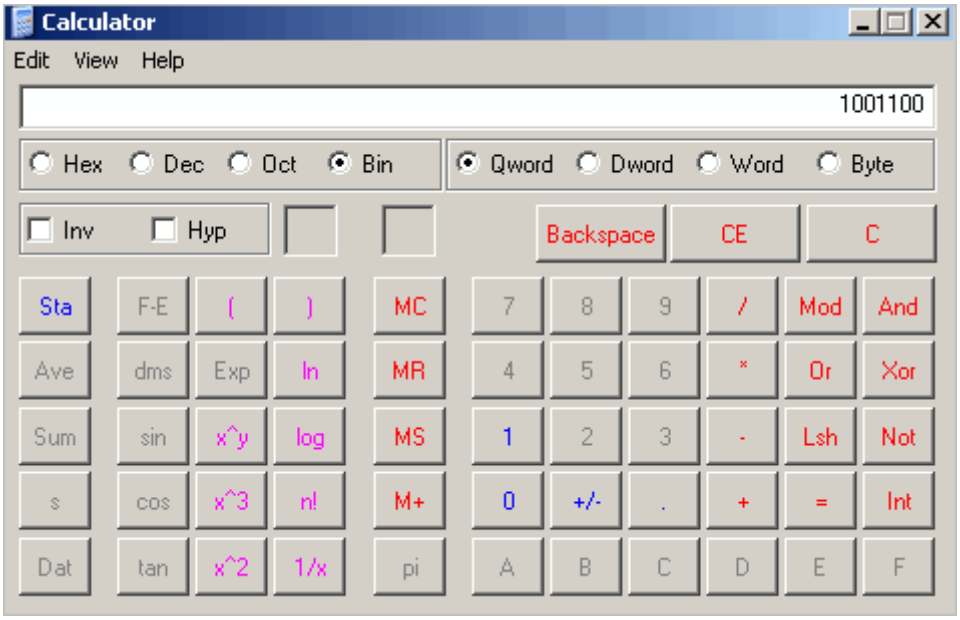
Hexadecimal digits have values ranging from 0 to F, which are represented as 0-9, A (for 10), B (for 11), etc. To convert a binary value (for example, 0100 1100) to a hexadecimal representation, treat the upper and lower four bits separately to produce a two-digit hexadecimal number (in this case, 4C).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

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

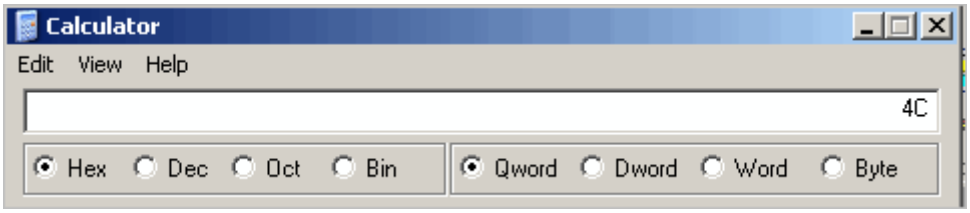
Scientific Calculator

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

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



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



Compliance Information

(according to ISO/IEC Guide 22 and EN 45014)

Manufacturer's Name & Address:
Lantronix 15353 Barranca Parkway, Irvine, CA 92618 USA

Declares that the following product:

Product Name Model: Device Server PRODUCT NAME

Conforms to the following standards or other normative documents:

Radiated and conducted emissions
Class B limits of EN 55022:1998
EN55024: 1998 + A1: 2001

Direct & Indirect ESD
EN61000-4-2: 1995

RF Electromagnetic Field Immunity
EN61000-4-3: 1996

Electrical Fast Transient/Burst Immunity
EN61000-4-4: 1995

Surge Immunity
EN61000-4-5: 1995

RF Common Mode Conducted Susceptibility
EN61000-4-6: 1996

Power Frequency Magnetic Field Immunity
EN61000-4-8: 1993

Voltage Dips and Interrupts
EN61000-4-11: 1994

Manufacturer's Contact:
Director of Quality Assurance, Lantronix
15353 Barranca Parkway, Irvine, CA 92618 USA
Tel: 949-453-3990
Fax: 949-453-3995

Warranty

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

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

* * * *

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

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

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

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

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